Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy

ANNUAL REPORT

TO PARLIAMENT 2002-2003

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy

ANNUAL REPORT

TO PARLIAMENT 2002-2003

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2003
Cat. No. IP30-1/2003
ISBN 0-662-67544-4

This publication is also available on our Web site at **www.privcom.gc.ca**

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Téléc.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

September 2003

The Honourable Daniel Hays, Senator
The Speaker
The Senate of Canada
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report for the Office of the Privacy Commissioner of Canada, for the period from April 1, 2002 to March 31, 2003 for the *Privacy Act* and from January 1 to December 31, 2002 for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

Robert Marleau
Interim Privacy Commissioner
of Canada

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Téléc. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

September 2003

The Honourable Peter Milliken, M.P.
The Speaker
The House of Commons
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report for the Office of the Privacy Commissioner of Canada, for the period from April 1, 2002 to March 31, 2003 for the *Privacy Act* and from January 1 to December 31, 2002 for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

Robert Marleau
Interim Privacy Commissioner
of Canada

103-07504/ .

Table of Contents

Foreword 1

Overview 3

Substantially Similar Provincial Legislation 13

Part One - Report on the *Privacy Act* 17

Introduction 17
Investigations and Inquiries 18
Complaints under the *Privacy Act* 19
Definitions of findings under the *Privacy Act* 21
Summary of select cases under the *Privacy Act* 22
Incidents under the *Privacy Act* 35
Public Interest Disclosures 37
Privacy Practices and Reviews 45
Privacy Impact Assessments 47
In the Courts 51

Part Two - Report on the *Personal Information Protection and Electronic Documents Act* 55

Introduction 55
Investigations and Inquiries 56
Definitions of findings under the *PIPED Act* 57
Summary of select cases under the *PIPED Act* 58
Incidents under the *PIPED Act* 83
Privacy Practices and Reviews 91
In the Courts 92

Part Three - Corporate Services 97

Foreword

My presenting this Annual Report for the fiscal year 2002-2003 may seem something of an oddity. I was appointed interim Privacy Commissioner in July of this year, well past the end of the reporting period, so I cannot take credit for any of the work that is reported here. But in fact this is less a real problem than it might seem. There is a lot more to the Office of the Privacy Commissioner than just the Commissioner, and even if I had been here for the entire time, it would be a fiction to call this "my" Annual Report. It reflects the work of very talented and dedicated individuals.

These are challenging times for the Office. For one thing, the task of protecting privacy has never been more arduous, what with new private sector legislation, a wide array of proposed anti-terrorist and security measures, and the increasing availability and sophistication of privacy-invasive technologies.

To complicate matters, the Office has undergone a period of intense public scrutiny and organizational disruption. The House of Commons Committee on Government Operations and Estimates conducted an inquiry into operational and administrative issues in the Office, and uncovered a number of

serious problems. As important and necessary as this exercise of Parliamentary oversight is, there is no denying that it, along with the accompanying media attention, has made it difficult for staff of the Office to conduct their work effectively.

I accepted the position of Privacy Commissioner on an interim basis in order to lead the Office through the process of rebuilding itself and repairing its relationship with Parliament and Canadians. Our task now is to regain the confidence of Parliament and our stakeholders, demonstrate to Canadians that they will receive top-level service in protection of their privacy rights, and ensure that organizations understand their obligations, and citizens their rights, when the *Personal Information Protection and Electronic Documents Act* comes fully into effect on January 1, 2004.

I have been impressed by the commitment of the Office's staff, and look forward to working with them in this exciting time. I am confident that from this period of renewal will emerge a new enthusiasm for the cause of privacy and a centre of excellence for its protection and promotion.

Overview

It is common to introduce an Annual Report with some remark about it providing an opportunity to reflect. In the case of this Report, that is not simply a throwaway introduction. The period under review has been an important one for privacy.

For one thing, privacy in our society has been in some danger. This of course is nothing new; privacy has never been something that we can take for granted, and particularly since the advent of computerization it has required active effort to preserve it. But if the danger to privacy is not new, it is intensified. The forces that have ground away at privacy for the last decade—technological advances in the collection, processing, matching, and analysis of personal information, growing pressure to identify and authenticate parties to electronic transactions, and the drive for security from crime and terrorism—have been particularly powerful in the last year.

Public security measures against crime and terrorism have certainly been the most acute and obvious challenge. They also present the most obvious challenge to privacy advocates and Privacy Commissioners, who must walk a fine line between protecting privacy and making life easier for criminals and terrorists.

But in fact the other forces threatening privacy are no less challenging, and arguing for privacy in the face of them often requires walking similar fine lines. Data matching catches people defrauding the system. Identity cards can make it harder for someone to fraudulently use your credit card. Electronic health records can facilitate diagnosis and treatment, and prevent costly or deadly medical mistakes. Giving researchers access to our personal health information can enable research that can prolong life and reduce suffering.

No one would argue with the goals of these measures. But privacy is not simply a frill or a selfish extravagance that can be tossed away the moment someone claims that it inhibits some other valuable social goal—regardless of whether the goal is security or public health or even individual life or death. Privacy is a cornerstone of individual freedom. It exists in a dynamic balance with our other social needs. The key to preserving privacy is careful analysis of any measure that purports to bring us some other social benefit, to ensure that the balance is maintained.

The results of our work in the past year have been mixed. We have continued to manage a large caseload of complaints and ensure that Canadians enjoy full protection of their rights under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. On more general questions of promoting and protecting privacy, we have made some important advances. We have also had some setbacks, and, on a couple of fronts, we have been forced to rethink our approach.

The Office achieved a successful outcome when it spoke up about the Canada Customs and Revenue Agency's proposed database about airline passengers.

On more general questions of promoting and protecting privacy, we have made some important advances.

This database, as initially proposed, was to contain extensive information on the foreign travel activities of Canadians--where

and with whom they travel, how they paid for their tickets, their contact addresses and telephone numbers, even their dietary and health-related requirements. The information would have been retained for seven years, and would have been available for a wide range of administrative and law enforcement purposes.

The impact of this would have been enormous, and unprecedented. The ordinary travel activities of law-abiding people, activities that previously would have passed unnoticed unless there were some reasonable grounds to suspect them, would have been recorded and retained, attached to their names. It would be one more loss of anonymity and privacy, one more way in which innocent people would be identified, tagged, and monitored by the state—in short, one more infringement of the right to privacy.

Our staff analyzed this proposal and concluded that the supposed security benefits to be gained did not justify the infringement of privacy that it represented. Our opposition, supported by public opinion, eventually led the Minister of National Revenue to revise the initiative, significantly reducing the impact on privacy.

One successful outcome does not make a great year. We continue to have concerns about other security initiatives, such as the provisions of the proposed *Public Safety Act* allowing the police to scan all airline passengers against outstanding arrest warrants, the "Lawful Access" proposals to enhance state powers to monitor electronic communications, the proposal for a national identification card, and the growth of police video surveillance of public streets.

One long-running dispute, about the confidentiality of census returns, appears headed for resolution in a manner that runs directly counter to the recommendations of our Office.

Canadians have been told at least since 1905 that the information they reveal in censuses will be held in confidence and only used for statistical purposes. The *Privacy Act* actually allows the National Archives to disclose personal

information collected in a census, 92 years after the information was collected. This remained largely academic until recently, because the only census records under the control of the Archives were those few that had been conducted up until 1901. Census officials took the view that, beginning with the 1906 census, regulations and legislation required them to keep the returns confidential rather than transfer them to the Archives.

Historians and other researchers have long sought access to these documents, and this year the government, following the recommendations of an expert panel but over our objections, released the 1906 census records and introduced legislation to allow the release of the rest.

Our Office had supported a compromise that would have limited access to the returns to scholars conducting peer-reviewed historical research and individuals wishing to conduct genealogical research on their own families. The government rejected this.

Our concern is with the repeated promises of confidentiality. Canadians were asked to reveal personal information to census-takers, and were led to believe that it would be kept confidential. Violating that promise could diminish the confidence Canadians have in government. We remain hopeful that this will be recognized when the House of Commons takes up this proposed legislation, which was passed by the Senate in May.

On another important privacy issue, video surveillance of public streets, we concluded that a new approach needs to be taken. The previous Commissioner had initiated a lawsuit in the British Columbia Supreme Court, alleging that the RCMP's video surveillance of a public street in Kelowna, B.C., violated the *Canadian Charter of Rights and Freedoms*. The Court, however, did not address the substance of the case at all. It ruled that the Privacy Commissioner simply does not have the capacity to launch such an action, and dismissed it on that basis.

This presented us with something of a quandary. On the one hand, video surveillance of public places has serious privacy implications, so the idea of simply

letting the issue drop because of a procedural problem seemed hardly satisfactory. On the other hand, regardless of what we wanted, the issue had become the one defined by the Court. If we had appealed the decision, the appeal would have been about that issue alone. To work our way through two more levels of appeal would have taken years, at the end of which we would have spent a great deal of the Office's energies and a considerable amount of public money, without any answer from a court on the substantive issue of video surveillance. The issue has to be addressed, but it must be done in a different way. Accordingly, we withdrew the case, but we will pursue this issue with determination.

It was striking this past year how many of our privacy concerns are tied up with anonymity and its opposite pole, identity.

It was striking this past year how many of our privacy concerns are tied up with anonymity and its opposite pole, identity. The ability to conduct the majority of our daily activities in an anonymous fashion is one of the keys to our keeping control of information about us. People can have a private life even if much of their lives is spent in public view, as long as their activities cannot be linked to each other and to themselves. It is the ability to connect activities to each other and to an identifiable person that is at the heart of profiling and surveillance.

This perspective ties together our concerns about such superficially different things as authentication of clients in electronic transactions, biometric facial recognition systems in airports, traveller databases, and a national identification card.

This was the view that we tried to impress upon the House of Commons Standing Committee on Citizenship and Immigration in its hearings on whether Canada needs a national identification card. We made the argument that such a card (whatever the details of the proposal are, and to date there is

no real proposal) would do little to address real problems, would present enormous financial and practical challenges to implement, and would do grave damage to privacy.

While the Office has wide-ranging interests and strives to serve as Parliament's window on all privacy issues, the heart and soul of its work is the system of enforceable privacy rights set up under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act.*

On this account, 2003 was a noteworthy year. First of all, it marks the 20th anniversary of the *Privacy Act*. That calls for reflection not just on the past year, but on the past twenty, and in particular on the model of privacy protection that Parliament adopted with the *Privacy Act*. That model is based around an Officer of Parliament, the Privacy Commissioner, who advises Parliament on privacy issues, analyzes the implications of legislative and regulatory initiatives so that Parliamentarians and Canadians can make informed decisions, and acts as an ombudsman to protect privacy rights, through negotiation, persuasion and dialogue—and occasionally, as a last resort, through publicity. The system set up under the *Privacy Act* quickly showed itself to be a useful one, and it was no surprise that it was adopted and applied to the private sector when Parliament passed the *Personal Information Protection and Electronic Documents Act.*

We are confident that in the past year, this system has proved useful to Parliament, and indeed has been reaffirmed. Parliament has rethought and revised legislative initiatives such as the CCRA database so as to minimize impacts on privacy, and we think that the outlook for privacy in Canada, despite all the pressures, is encouraging.

The year 2003 is important for the other statute we administer, the *Personal Information Protection and Electronic Documents Act* or *PIPED Act* as we call it, since this is the last year before it reaches its full application. The Act has been coming into force in stages. At the outset, in 2001, it applied to certain commercial exchanges of information but excluded personal health information. As of January 2002, it extended to include personal health information. The

final stage will begin in January, 2004, when the Act will apply to all commercial activity in Canada except where provinces have passed substantially similar legislation. (To date, only Quebec has privacy legislation deemed substantially similar, but both British Columbia and Alberta introduced legislation this year, another promising sign for privacy protection in Canada.)

In general, the introduction and implementation of the Act have gone far more smoothly than some had predicted. The business community has responded well to the demands of complying with the legislation, and while there have been some bumps in the road, on the whole the new way of doing business has not been as difficult or traumatic as some had predicted. We are seeing a general recognition that respecting privacy is not as onerous as some people thought, and in fact is simply good business practice. One of the most encouraging signs is the obvious interest in compliance among the business community. In fact, a sort of compliance cottage-industry has sprung up, with a host of consulting firms offering expertise in compliance with the Act. Hardly a week goes by without our receiving a brochure for a seminar or workshop about the *PIPED Act*.

And the ombudsman model, which proved itself under the *Privacy Act*, has also worked well with respect to the *PIPED Act*. We have been encouraged by the willingness of private sector organizations subject to the Act to comply with the requirements in the legislation and to recognize the Office's specific expertise in getting to the bottom of privacy issues.

We are seeing a general recognition that respecting privacy is not as onerous as some people thought, and in fact is simply good business practice.

As far as day-to-day operations are concerned, the Office continued to face significant challenges, but it remains a resilient and healthy organization in the face of heavy public demand for its services. We

dealt with a heavy caseload of complaints under the *Privacy Act*, including a 35% increase in new complaints over last year. Under the *PIPED Act*, the number of new complaints almost tripled over last year, and we can expect a significant increase with the extension of the application of the Act in 2004.

An important development in the past year was the introduction of the Treasury Board's new policy on privacy impact assessments.

A privacy impact assessment, or PIA, is quite simply an assessment of how, and how much, a program or activity affects the privacy of individuals. Typically, it will entail a description of the program, an analysis of what will happen to the personal information collected, used, and disclosed, and an assessment of the program's compliance with privacy principles, legislation, and policies. The Treasury Board's new policy makes PIAs a condition of funding for all new, substantially redesigned, or electronically driven programs and services that collect, use, or disclose personal information. Canada is the first country in the world to make PIAs mandatory in this way.

The implementation of this policy means that government institutions will have to look at privacy right from the outset, from the moment they begin planning a new program. The significance of this is that questions of whether a program or project has a negative effect on privacy—whether it will entail new data matching or increased sharing of personal information, for example, or result in the development of new common personal identifiers, or extended use of existing ones—will be asked before any privacy violation occurs. This preventive approach, rather than a punitive or remedial one, is the most sensible approach to an issue like privacy. Once privacy is violated, once an individual's personal information has been taken out of his or her control, it cannot be undone. Lost privacy cannot be given back. That is why Treasury Board's policy is so

So it has been a year of some good news, some disappointments, and many continuing challenges.

welcome. When government initiatives add to sound governance, it should be recognized and applauded.

So it has been a year of some good news, some disappointments, and many continuing challenges. Fortunately, we have not had to face all our challenges alone. The protection of privacy involves us in a continuing dialogue, in Canada and abroad, with privacy advocates, civil libertarians, academics, and, of course, other privacy and data protection commissioners. They have helped us to bear the burden of the disappointments, and they deserve full credit for their part in bringing about the good news.

The Standing Committee on Government Operations has done its duty in holding this Office accountable to higher standards of prudence and probity in the use of public funds. As we move forward in another watershed year for privacy issues, the Office of the Privacy Commissioner will work for renewed support from the Senate and the House of Commons to blunt the impact of pervasive and invasive technologies and policies on the privacy rights of Canadians.

Substantially Similar Provincial Legislation

Under paragraph 26(2)(b) of the *Personal Information Protection and Electronic Documents Act*, the Governor in Council can exempt an organization, a class of organizations, an activity or a class of activities from the application of *PIPED Act* with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation deemed to be substantially similar to the *PIPED Act*.

The intent of this provision is to allow provinces and territories to regulate the personal information management practices of organizations operating within their borders, provided that they have in place a law that is substantially similar.

If the Governor in Council issues an Order declaring a provincial act to be substantially similar, the collection, use or disclosure of personal information by organizations subject to the provincial act will not be covered by the *PIPED Act*. Personal information that flows across provincial or national borders will be subject to the *PIPED Act* and the *PIPED Act* will continue to apply within a province to the activities of federal works, undertakings and businesses that are under federal jurisdiction such as banking, broadcasting, telecommunications and transportation.

On September 22, 2001, Industry Canada published a notice in the *Canada Gazette* Part 1 setting out the process that the department will follow for determining whether provincial/territorial legislation will be deemed substantially similar.

The process will be triggered by a province, territory or organization advising the Minister of Industry of legislation that they believe is substantially similar to the *PIPED Act*. The Minister may also act on his or her own initiative and recommend to the Governor in Council that provincial or territorial legislation be designated as substantially similar.

The Minister has stated that he will seek the Privacy Commissioner's views on whether or not legislation is substantially similar and include the Commissioner's views in the submission to the Governor in Council.

The process also provides for an opportunity for the public and interested parties to comment on the legislation in question.

According to the *Canada Gazette* notice, the Minister will expect substantially similar provincial or territorial legislation to:

- incorporate the ten principles in Schedule 1 of the *PIPED Act*;
- provide for an independent and effective oversight and redress mechanism with powers to investigate; and
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

The process also provides for an opportunity for the public and interested parties to comment on the legislation in question.

In addition to providing comments to the Minister of Industry with respect to specific provincial or territorial legislation, the

Privacy Commissioner is required by subsection 25(1) to report annually to the Parliament of Canada on the "extent to which the provinces have enacted legislation that is substantially similar to the *PIPED Act*."

The previous Commissioner issued two reports to Parliament on the matter of substantially similar provincial legislation. In May 2002, he issued a report in which he concluded that Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* is substantially similar to the *PIPED Act* in terms of the extent to which it protects personal information. In June 2003, the previous Commissioner issued a second report in which he raised concerns about Bills 44 and 38 that have been introduced, but not yet passed, by the provinces of Alberta and British Columbia, respectively.

As neither Bill has been passed, we will continue to monitor their progress and maintain a dialogue with our provincial counterparts.

Part One

Report on the *Privacy Act*

INTRODUCTION

The *Privacy Act*, which has been in force since 1983, protects individuals' privacy with respect to personal information held by federal Government institutions. The *Act* governs how federal institutions collect, use, disclose and dispose of personal information, and it gives individuals rights to request access to and correction of their personal information. It also sets out the Privacy Commissioner of Canada's duties, responsibilities and mandate.

The Privacy Commissioner receives and investigates complaints from individuals who believe their rights under the *Act* have been violated. The Commissioner can also initiate a complaint and investigation himself, in any situation where there are reasonable grounds to believe the *Act* has been violated.

As an ombudsman, the Commissioner's first priority is to resolve complaints to the extent possible, through mediation and negotiation if that becomes necessary. But the *Act* also gives the Commissioner broad investigative powers – he can subpoena witnesses and compel testimony, enter premises to obtain documents and conduct interviews. Obstructing an investigation is an offence under the *Act*. While the *Act* does not grant the Commissioner any order-making powers, the Commissioner can recommend changes to the way

Government institutions handle personal information, based on findings in a complaint.

The Commissioner also has a mandate to conduct periodic audits of federal institutions and to recommend changes to any practices that he considers not being in compliance with the *Privacy Act*.

The *Act* requires the Commissioner to submit an Annual Report to Parliament on the activities of his Office in the previous fiscal year. The current Report covers the period from April 1, 2002 to March 31, 2003 for the *Privacy Act*.

INVESTIGATIONS AND INQUIRIES

The Office's Investigations and Inquiries Branch is responsible for investigating complaints received from individuals under section 29 of the *Privacy Act* (and section 11 of the *Personal Information Protection and Electronic Documents (PIPED) Act*, which is discussed later in this Report).

Essentially, these investigations serve to establish whether individuals have had their privacy rights violated and whether they have been accorded their right of access to their personal information.

Where privacy or access rights have been violated, the investigation process seeks to provide redress for individuals and prevent violations from reoccurring.

The *Privacy Act* gives the Commissioner the authority to administer oaths, receive evidence and enter premises where appropriate, and examine or obtain copies of records found in any premises.

We are pleased to note that we have had voluntary co-operation to date, and all complaints brought before the Commissioner and his predecessors have been resolved without having to use these formal investigative powers.

The Investigations and Inquiries Branch also responds to thousands of inquiries annually from individuals and organizations contacting the Office for advice and assistance on a wide range of privacy-related matters.

Complaint Investigations Closed
April 1, 2002 to March 31, 2003

2001-2002:	1,673
2002-2003:	3,483

COMPLAINTS UNDER THE *PRIVACY ACT*

During the current reporting year, this Office received 1,642 new complaints. Approximately 43% were filed by individuals alleging that their access rights under the *Privacy Act* had been violated; 24% concerned allegations that the confidentiality provisions of the *Act* with regard to collection, use, disclosure, retention and disposal of personal information had not been respected; and the remaining 33% were about the tardiness of Government institutions in responding to requests for access to personal information.

More than two-thirds of the total received were lodged against five federal Government institutions – Correctional Service of Canada, the Canada Customs and Revenue Agency, the Royal Canadian Mounted Police, the Department of National Defence, and Citizenship and Immigration Canada.

The former Commissioner issued findings on 3,483 complaints during the year. It is important to note that this figure includes 2,323 complaints related to the Canada Customs and Revenue Agency's (CCRA) disclosure of personal information on Customs' E-311 declaration cards to Human Resources Development Canada (HRDC).

At issue was whether there was sufficient authority to justify the use of personal information collected by the CCRA for one purpose – to declare goods

a traveller is bringing into Canada – for use by HRDC for a totally unrelated purpose – in an investigative data match program to identify returning travellers who were fraudulently receiving employment insurance benefits while outside the country.

The matter had been referred to the Court for an opinion on whether the disclosure was authorized by section 8(2)(b) of the *Privacy Act* and section 108 of the *Customs Act* and whether the use of that information by HRDC as evidence against the individuals contravened their rights under the *Canadian Charter of Rights and Freedoms*.

The Supreme Court of Canada ruled that the disclosure was permissible based on its interpretation of these provisions of the *Privacy Act* and the *Customs Act*. The Court also upheld the lower Court's decision that, based on the limited nature of the information disclosed, there was no reasonable expectation of privacy and as a consequence travellers had not been denied their right under the *Charter* to be secure from unreasonable search or seizure. On that basis, the former Commissioner was required to report to the complainants that their complaints were not well-founded.

Of the remaining 1,160 completed cases, 486 dealt with access matters, 293 dealt with collection, use, disclosure, retention and disposal of personal information, and 381 dealt with time limits. The 3,483 complaints were concluded as follows:

Not well-founded	2,711
Well-founded	371
Well-founded/resolved	77
Resolved	13
Settled	235
Discontinued	76

DEFINITIONS OF FINDINGS UNDER THE *PRIVACY ACT*

Not Well-founded: A finding that a complaint is *not well-founded* means that the investigation uncovered no evidence to lead the Commissioner to conclude that the Government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: A finding that a complaint is *well-founded* means that the Government institution failed to respect the *Privacy Act* rights of an individual. This would also be the Commissioner's finding in a situation where the Government institution refuses to grant access to personal information, despite our recommendation that it be released. In such a case, the next step could be to seek a review by the Federal Court of Canada.

Well-founded/Resolved: The Commissioner will find a complaint to be *well-founded/resolved* when the allegations are substantiated by the investigation and the Government institution has agreed to take corrective measures to rectify the problem.

Resolved: *Resolved* is a formal finding that reflects the Commissioner's role as an ombudsman. It's for those complaints where *well-founded* would be too harsh to fit what essentially is a miscommunication or misunderstanding. It means that this Office, after a full and thorough investigation, has helped negotiate a solution that satisfies all the parties.

Settled during the Course of the Investigation: This is not a formal finding but an acceptable means to dispose of a complaint when the investigation is completed, and the complainant is satisfied with the efforts of this Office and doesn't wish to pursue the issue any further. The complainant retains the right to request a formal finding. When that happens, the investigator reopens the file, and submits a formal report, and the Commissioner reports the findings in a letter to the complainant.

Discontinued: This means that the investigation was terminated before all the allegations were fully investigated. A case may be *discontinued* for any

number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion. The Commissioner does not issue a formal finding in discontinued complaints.

SUMMARY OF SELECT CASES UNDER THE *PRIVACY ACT*

CIC was collecting income tax information from Canadian employers

Three individuals who wished to employ live-in caregivers from the Philippines complained to this Office that the Canadian Embassy in Manila was asking them to provide sensitive income tax information before it would issue visas to their prospective caregivers. The individuals were worried about sending tax documents containing their social insurance numbers (SINs) and detailed information about their financial situation to a foreign country, especially with identity fraud having become such a major concern.

Citizenship and Immigration Canada (CIC) explained that the Live-In Caregiver Program (LCP) brings qualified caregivers to Canada in situations where there are no Canadians or permanent residents available to fill certain positions. Canadians wishing to hire a caregiver from abroad are required to have their job offer validated through Human Resources Development Canada (HRDC) and to sign a form declaring that they can financially support the person they will employ.

After the job offer was validated by HRDC, the Visa Section of the Canadian Embassy in Manila asked the prospective employers to send their Notice of Assessment for the last two years, their T-4 slips and a letter from their employer confirming employment.

CIC claimed that the information was necessary to determine the *bona fides* of an employment offer and to confirm that the employers were financially capable of supporting a caregiver.

When questioned about its authority to collect income tax information for the purpose of issuing visas to third parties, CIC referred to section 203 of the *Immigration and Refugee Protection Regulations*. A review of that document indicated that the visa officer must determine if the job offer is genuine and if the employment of the foreign national is likely to have a neutral or positive economic effect on the labour market in Canada.

In the previous Annual Report, the former Commissioner stated his position concerning the collection of income tax information without legislative authority. He explained that he found it untenable that an income tax return can be demanded from an individual for a purpose other than that required by law. Canadians should never be required to compromise a fundamental right in order to do business with the Government.

This Office presented those arguments to CIC and, as a result, the Embassy in Manila confirmed that it has ceased asking for income tax information for the purpose of issuing visas to live-in caregivers.

CCRA collected medical information for tax purposes

We received a complaint from a family who alleged that the Canada Customs and Revenue Agency (CCRA) had improperly collected their personal information from a provincial medical insurance plan. The family moved to Africa for three years and before leaving Canada the husband consulted with the CCRA and was told that, for tax purposes, he would be considered a non-resident during his absence from the country. Yet upon returning to Canada he was told that he did not meet the requirements for non-resident status and was taxed accordingly. He later obtained his personal information following a *Privacy Act* request to the CCRA and learned that it had asked the provincial insurance provider for all medical records about him, his wife and his children—including records originating some eight months prior to their departure for Africa and almost 2 1/2 years after their return to Canada.

We established that in order to qualify for non-resident status for tax purposes the CCRA must be satisfied that an individual has sufficiently severed ties

with Canada after moving to another country. The CCRA relies on provisions of the *Income Tax Act* as its authority to obtain sufficient information in order to assess non-residency status. It routinely conducts inquiries when assessing an individual's status, including verifying whether the individual continues to make claims under a provincial medical insurance plan during the time absent from Canada. The fact that an individual made such a claim could be an indication that all ties with Canada had not been severed.

The former Commissioner was satisfied that the CCRA had the necessary authority under the *Income Tax Act* to collect personal information about each family member from the province in order to make a determination on their residency status. Nevertheless, he was concerned about the *extent* of the medical information collected, particularly the information for the periods of time both before the family left the country, and after it returned. CCRA officials did not disagree with the concern that requesting medical information for the 2 1/2-year period after the family's return was excessive.

Under the circumstances, the former Commissioner determined that the CCRA collected more personal information than was necessary and, as a result, had exceeded its authority under section 4 of the *Privacy Act*. He found the complaints well-founded and recommended that the CCRA destroy the information that it obtained from the province.

Inadvertent disclosure of sensitive medical information by ATIP

Personal health information – information about the state of our bodies and minds – is arguably the most private information of all. When that information is not treated with the utmost care and confidentiality, the consequences can be disastrous. A case in point: an individual submitted an *Access to Information Act* (*ATIA*) request to a Government institution for all documents concerning the appointment of another Government employee to a specific position. The names of the two individuals were only vaguely similar. Yet because the departmental Access to Information and Privacy (ATIP) office's analyst had not taken care to properly read the individuals'

names when processing the *ATIA* request, an assumption was made that the requester and the appointee were one and the same individual. Thus, virtually all the information in the staffing file was disclosed to the *ATIA* requester – a small amount of third party information was removed. The file contained information about the appointee that was extremely private in nature – extensive medical and financial information, information about his family, his own employment and education history, and his home address and telephone number. It was also discovered that there was an uncomfortable history between the two individuals and that the requester had subsequently used some of the appointee's medical information to conduct his own personal inquiries about the appointee.

When that information is not treated with the utmost care and confidentiality, the consequences can be disastrous.

Following an investigation the institution readily admitted the error, apologized to the individual for what had occurred and gave him a copy of the same package the requester received so that he could see exactly what information about him had been improperly disclosed. The institution also asked the requester to return the information and to not keep any copies of it. While he returned the information, there were no assurances that copies had not been kept. Even had assurances been given, the damage had already been done and the appointee's personal information had already been further disclosed by the requester.

The former Commissioner accepted the fact that the situation occurred as a result of careless human error, but was appalled that the mistake was made at all – especially by the very people within the institution who are supposed to be the resident experts on the protection of personal information. Had the appointee's personal information been reviewed with the care it deserved this grievous violation of his privacy rights would never have occurred.

Disclosure of criminal past to offender's family members

An individual complained to this Office that a Correctional Service Canada (CSC) employee disclosed information about his criminal past to members of his family (including his young children who were previously unaware of their father's past) and to the public. A number of years ago the individual had been incarcerated in the same federal institution where the officer worked and he alleged that the officer disclosed confidential information obtained in the course of his duties.

The individual had also filed a complaint with CSC, which in turn conducted its own investigation. From the outset, the complainant never wavered in his statements that the officer disclosed his personal information. The officer maintained that it was not he who made the remarks, but rather a friend who was present at the time the disclosure took place – an individual he refused to identify either to us or to CSC. All of our efforts to locate the friend met with negative results. Still, based on all of the information we gathered during our investigation, the former Commissioner was prepared to find that the rights afforded the complainant under the *Privacy Act* had been violated as a direct result of the officer's actions. Indeed, CSC concluded that the officer had contravened its Code of Discipline and that he failed to observe the provisions of the *Privacy Act*; he was subsequently suspended for 15 days without pay.

Before rendering his final decision in the matter, the former Commissioner questioned CSC's rationale for concluding that a three-week suspension was appropriate to the circumstances. It was only then that we learned that new developments in the case had caused CSC to reverse its decision and withdraw the officer's suspension. Given the disciplinary action meted out to the officer, his friend had come forward saying that it was he who had disclosed the complainant's personal information, not the officer. While not fully convinced of the friend's credibility – and despite apprehensions in that regard – CSC nevertheless withdrew the suspension.

In light of this new information we conducted further inquiries but found no reason to believe the friend's version of events. Based on the evidence we

obtained, the former Commissioner concluded that it was the officer who disclosed the individual's personal information and that his friend likely only came forward because the repercussions to the officer turned out to be greater than anticipated. The former Commissioner therefore found the complaint well-founded and asked that CSC reconsider the reversal of its decision.

The former Commissioner also advised CSC that it should have advised our officials that the officer's friend had finally come forward after all of the attempts of both CSC and this Office had failed to find him. The former Commissioner considered this to be an extremely important development, one which caused CSC to reverse its initial decision and one which could obviously have had a direct bearing on his decision. CSC was well aware that we had an active investigation into the allegations made by the complainant and, in the former Commissioner's view, CSC should have immediately alerted our officials to the change of events. The former Commissioner received assurances that this was an isolated incident which would not reoccur.

Even a public record should be protected

An individual received an envelope, by courier and addressed to him, containing the Canada Pension Plan (CPP) appeal documents of another individual. He believed that the other individual must have received his own appeal information in error.

Our investigation into this matter confirmed these fears. The other individual had indeed received the complainant's appeal information from HRDC. The mix-up was the result of a lack of attention when the documents were inserted in the envelopes to be sent out.

Section 8 of the *Privacy Act* limits how Government institutions may disclose personal information. In essence, institutions may not disclose personal information to third parties without the consent of the person to whom the information relates, unless one of the permitted disclosures set out in section 8(2) of the *Act* applies.

HRDC explained that the information about the complainant that was disclosed consisted of documents that had been filed at the Federal Court and thus were part of a public record. Since section 69(2) of the *Privacy Act* states that section 8 does not apply to personal information that is publicly available, HRDC contended that it had not contravened the *Act* by sending out the information to the wrong individuals by mistake.

The former Commissioner disagreed because the complainant's information was not disclosed from a public record. The fact that it could be found in a public record does not negate the fact that HRDC disclosed the complainant's information to someone who had no need to know. On that basis, the former Commissioner concluded that the complaint was well-founded.

As a result of the complaint, HRDC apologized to the individuals, re-sent to them the information that had been misdirected and revised its mailing procedures to minimize the chances of a reoccurrence.

Unauthorized disclosure of a SIN

We investigated an individual's complaint that Human Resources Development Canada (HRDC) improperly disclosed his social insurance number (SIN) to a private investigator.

The complainant had filed a lawsuit against an insurance company that he believed had mishandled his insurance claim. During the court process he discovered that the insurance company had hired a private investigator to delve into his financial affairs. He obtained a copy of the investigator's report, and noted references to inquiries conducted at HRDC, and the information obtained as a result of those inquiries. Dissatisfied because of HRDC's apparent lack of willingness to address his concerns about this breach of his privacy, the individual eventually turned to this Office for assistance.

We established during the investigation that an employee of HRDC had queried the complainant's file in the Social Insurance Register (SIR) system during the same time period that the private investigator had conducted his inquiries. Although the complainant reported his concerns to HRDC, it did

not pursue the matter further until he indicated that he intended to subpoena HRDC employees to testify in court in his suit against the insurance company. At that time he asked for a copy of HRDC's investigation file concerning the disclosure of his SIN and any information related to the action taken by HRDC in that regard. It was only at this point – almost ten months after he first reported his concerns – that HRDC decided to conduct an internal inquiry to determine whether, or how, his SIN may have been compromised.

Dissatisfied because of HRDC's apparent lack of willingness to address his concerns about this breach of his privacy, the individual eventually turned to this Office for assistance.

It was clear from the evidence obtained during our investigation that the HRDC employee had obtained access to the individual's SIN without justification and disclosed it to the private investigator. The evidence also pointed to the possibility that the employee had also gained access to approximately 40 other client files on the SIR system for which there were no related HRDC case files that would require the employee to query their SIN files.

The former Commissioner was concerned with HRDC's lack of conviction in handling the individual's complaint about the disclosure of his SIN when he first brought it to their attention. They failed to take any action other than to issue him a new SIN, despite the fact that several officials were aware of the incident long before he complained to this Office. The former Commissioner was equally concerned that despite the seemingly adequate systems capabilities, HRDC managers do not routinely monitor the SIR system to identify and deal with any activities of a suspicious nature or that cannot otherwise be justified as part of an employee's duties.

The former Commissioner concluded that HRDC was responsible for its employee's improper disclosure of the individual's SIN to the private investigator, and that it had as a result contravened the confidentiality provisions of the *Privacy Act*.

In response to this finding, HRDC undertook to mitigate the damage to the extent possible. The Deputy Minister sent a letter of apology to the complainant, and implemented measures that will significantly enhance the security of personal information in the SIR database, and enhance monitoring of employees' access to the SIR. We are confident that this will improve HRDC's abilities to protect the personal information under its control and prevent any further violations of client privacy.

HRDC also decided to refer the matter to the Royal Canadian Mounted Police for criminal investigation – the employee was eventually fired by HRDC for the breach of security.

Statistics Canada census taker not responsible for disclosing personal information to banks

An individual alleged that Statistics Canada sold her name and address to financial institutions that then sent her unsolicited mail. The individual travelled frequently for extended periods and maintained a post office box. She was staying at a recreation vehicle park at the time of the 2001 census and the census taker explained to the individual that she would have to use the park address for the purposes of the census, which she did. Within a couple of months, she began to receive unsolicited mail addressed to her at the park. As she had only used that address for the census, it seemed logical to her that Statistics Canada must have sold or otherwise provided the address to the financial institutions.

We examined one solicitation that the individual had received and contacted the bank that had sent it to her. Using the code displayed on the form letter, the bank was able to determine that it had obtained her name and park address from one of the largest list management companies in Canada, which

handles more than 500 mailing lists representing some 25 million names. Its officials confirmed that the complainant's information was contained on one of the mailing lists which had been created and updated from information obtained from provincial telephone companies across Canada.

This detail prompted the individual to recall that she had a telephone installed at the park. While her telephone bill was sent to her post office box address, she had to provide the telephone company with the address of the park in order to have the telephone installed and serviced. It became apparent that it was the telephone company and not Statistics Canada that had disclosed the individual's name and address to the list broker, which in turn provided her information to the banks.

During the investigation, the list broker was asked to remove the individual's name from the mailing list, which it did immediately. However, the individual was alerted to the possibility that while her name would not be on an updated list, old lists held by the list broker's customers might still contain her information, and thus she might continue to receive solicitations. The former Commissioner urged her to contact those companies directly in order to remove her name from those lists. He also reminded the complainant that her name could be included in other lists in the future if, for example, she applies for credit cards, completes contest forms or purchases magazine subscriptions.

Time Limit Complaints

Under the *Privacy Act*, Canadians have a right of access to their personal information held by Government institutions and, by law, institutions must respond within 30 days after the request is received. Institutions can, however, extend that time limit to a maximum of an additional 30 days, but only under two specific circumstances: if meeting the 30-day time limit would unreasonably interfere with the institution's operations, or if consultations are required which cannot reasonably completed within that time.

The number of complaints related to time limits being exceeded by federal institutions for providing personal information to citizens increased to 541

this year, compared to the 428 that were reported for the previous fiscal year. We closed 381 of these complaints, of which 302 were well-founded.

There were more complaints about the personal information-handling practices of Correctional Service Canada (CSC) than any other federal Government institution. Of the 177 complaints against CSC that we completed, 159 were well-founded. Although CSC increased its staff and streamlined its procedures, a delay problem in responding to requests for personal information continues.

The number of time limit complaints against two institutions dropped significantly in comparison to last year, whereas those against four others increased:

Canada Customs and Revenue Agency:	down from 85 to 31
Human Resources Development Canada:	down from 57 to 16
Correctional Service Canada:	up from 125 to 233
Royal Canadian Mounted Police:	up from 16 to 71
Department of National Defence:	up from 35 to 58
Citizenship and Immigration Canada:	up from 40 to 49

One factor that continues to hamper the ability of institutions to respond to requests within the prescribed time limits is the complexity of processing audio and videotapes.

Institutions sometimes record interviews conducted for administrative or criminal investigations. Since the *Privacy Act* applies to personal information that is "recorded in any form," individuals can ask for copies of their information on those tapes. It is a time-consuming process to listen or view tapes and then to identify and sever the information that requesters are not entitled to receive, often because it constitutes personal information about other individuals. The Department of National Defence is one of the organizations that records interviews, and it has recently acquired new equipment in an attempt to simplify the process of reviewing and severing information on tape.

Requests for voluminous investigation files also account for some delays in responding in a timely manner.

Transmittal of information by fax

Although we discourage institutions from sending personal information by fax, we realize that they are used regularly by institutions for the purposes of expediency in getting information to its destination.

One of our investigations uncovered a problem with the manner in which a Government institution was keeping a record of the personal information it was sending by fax. Fax cover sheets indicated the number of pages sent, to whom, by whom and on what date, but the institution could not identify, after the fact, which specific documents or pages had been transmitted. In other cases, the institution was not able to identify what it had received by fax from other areas in the institution.

It is imperative that institutions keep a record of the use and disclosure of personal information under their control. Except in limited circumstances, individuals have the right to know which documents containing their personal information are sent to whom and why they are disclosed.

A solution to this problem is to list the documents sent or received on the transmittal cover sheet itself. This will ensure transparency, document the flow of information and assist us in our investigations.

Processing original files versus photocopies

Some Government institutions have denied individuals access to their personal information, thus contributing to the rising number of complaints to this Office, because the departmental Access to Information and Privacy (ATIP) offices are increasingly relying on photocopies provided by their program areas, rather than working with original documents, when processing requests. The problem with this arrangement is that ATIP analysts cannot be certain that what they are given represents all the information the individual is seeking.

When this Office receives a "denial of access" complaint, we ask to see the original file to compare it with the information processed by the ATIP office. Often we have discovered that the ATIP office did not have all the information contained on the original file-because someone did not think it was relevant or had removed internal notes, or simply because the backside of double-sided documents had been missed when the documents were photocopied.

The subtle nuances that can only be appreciated when viewing original files are also lost. Photocopies do not reveal the use or meaning of different coloured forms or highlighting of significant passages, and may not capture the exact placement of post-it notes with comments. Nor do they include the paperclips that explain why certain documents are grouped together or why they are out of chronological order. These elements are essential to understanding the context of the file and to decide whether the personal information can be released to the individual.

Having our investigators review original files eliminates any misgivings that the institution may not have located all the requested information, and also gives us the unequivocal certainty that we require to ensure access has not been denied.

Although some program areas would rather not surrender their original files, particularly those with ongoing administrative activities, we suggest that they retain a photocopy for their own use for the few days it takes the ATIP office to review the original file. We also urge ATIP co-ordinators to reclaim their responsibility for the quality of responses they send to individuals by working with original files only.

INCIDENTS UNDER THE *PRIVACY ACT*

Incidents of mismanagement of personal information that warrant further review by this Office are sometimes brought to our attention. We conducted 32 such reviews last year.

As an example, last summer, following an office relocation from one building to another in Ottawa, Human Resources Development Canada's (HRDC) Disability and Benefits Appeal Branch staff discovered that two computers were missing. Although HRDC, following an investigation by its Security Division, was unable to determine exactly what had happened, it is believed that the computers were stolen when they were left unattended while waiting to be loaded into the moving trucks. It has been suggested that since both computers were new, they were taken because of their monetary value and not for what they contained. The theft was also reported to local police, but they were unable to find the missing computers or the perpetrators.

Our investigators ascertained that the computers had not been packed in boxes, but simply placed on moving trolleys without being secured in any way. They also determined that one HRDC employee was responsible for ensuring that all items were removed from their original location to the loading area, but no one actually supervised the physical transfer of items from that location to the moving trucks parked outside the building.

Although the computers were never found, HRDC was able to determine, by means of back-up computer tapes, that they contained the full names, social insurance numbers (SINs) and medical information of dozens of Canada Pension Plan (CPP) disability benefits recipients. Therefore, HRDC decided to notify those recipients about the theft.

During our review of the incident, however, we noted that an additional 38 individuals whose surnames and SINs appeared on documents had not been notified. Since this would be sufficient personal information to possibly identify these individuals, we asked HRDC to notify them of the theft as well, which it did.

We also recommended that HRDC implement additional security measures to ensure that this does not reoccur, specifically that it ensure that all personal information is removed from hard drives of computers before they are moved from one location to another; and that additional staff be present during moves to ensure adequate security for any personal information that is affected by the move.

In another incident, an individual informed this Office that documents he received from a small claims court relating to his suit against a Port Authority included personal information relating to other individuals, specifically their credit card account numbers.

Our staff determined that when the Port Authority filed its Statement of Defence in small claims court, it included a copy of a daily cash and deposit report and a cash deposit receipt. These documents identified other individuals along with their account numbers, invoice numbers, credit card numbers, and amounts paid to the Port Authority.

In its defence, the Port Authority believed that it had no choice but to file complete, unvetted documents with its Statement of Defence to comply with court procedures. As part of its defence it needed to present the information relevant to its financial transactions with the plaintiff, and was under the impression that it could not remove any information relating to the other individuals named in those documents.

When this Office made inquiries with the small claims court, we learned that it would in fact accept partial or severed documents. The Port Authority therefore could have removed all information not relating to the plaintiff when it filed its documents in court, including the personal information about the other individuals. We brought this matter to the attention of the Port Authority and, as a result, it has undertaken to have the information relating to the other individuals removed from the court's file. The Port Authority also contacted the concerned individuals to advise them that their personal information was included in a public record.

PUBLIC INTEREST DISCLOSURES

Paragraph 8(2)(m) of the *Privacy Act* allows the head of a Government institution to disclose personal information without an individual's knowledge or consent if there is a clear overriding public interest in doing so – either because it outweighs the individual's right to privacy or because it would clearly benefit the individual. Under section 8(5) of the *Act*, the Privacy Commissioner is to be notified in advance of any proposed disclosures.

This past year, the former Commissioner reminded a couple of institutions, following a review of their notifications, that the discretion to disclose personal information in the public interest should occur on an exceptional basis, where the disclosure cannot be justified under any of the other permissible disclosure provisions found in the *Act*.

It had become increasingly evident that some institutions were using the provision on a systematic and routine basis, with little apparent thought as to whether there was indeed an overriding public interest at the time. This was troubling because the situation seemed to play little or no part in the decision-making process. Often there had been no evaluation to assess what was of public interest and whether that interest should override the individual's privacy rights. As an individual rarely, if ever, has a chance to challenge the decision, it is critical that the decision-makers act in a judicious manner and ensure they have all the relevant information before making a fair determination.

However, of the 70 public interest disclosure notifications we received during the year, one was clearly warranted: the decision of the Department of National Defence (DND) to share with Veterans Affairs information regarding approximately 2,500 individuals involved in chemical warfare experiments.

From World War II to 1992, Defence Research and Development Canada (DRDC), a branch of DND formerly known as the Defence Research Establishment, compiled a list of DND members it had exposed to various

chemicals as part of its chemical warfare research program. The members were volunteers, but some may not have been aware they were part of the experiments.

As a result of a recent investigation by the Office of the Military Ombudsman, DND felt that the DRDC's information would be useful to Veterans Affairs in identifying veterans who could be entitled to benefits. The information included the individual's last name and initials, the name of the chemical administered, the date administered and the location. It also included some service numbers but no dates of birth, which left it impossible for DND to positively match all of the individuals to its employee records.

The DRDC had not copied this information to the service or medical files of the affected employees, and DND hoped that Veterans Affairs would compare the information with its records to identify any matches in its inventory, and get in touch with the individuals. The intent was that Veterans Affairs could review the cases of those veterans who claimed to have been exposed to noxious substances, including anthrax, but were refused financial assistance because there was no evidence on their service or medical files to support their claims.

The former Commissioner readily agreed with DND's decision. The benefit to the individuals was evident-Veterans Affairs could help to resolve benefit entitlement issues as well as to assist in the diagnosis and treatment of disease resulting from exposure to toxic substances.

Top Ten Departments by Complaints Received

April 1, 2002 to March 31, 2003

Organization	Total	Access to Personal Information	Time	Privacy	Other
Correctional Service of Canada	456	106	233	117	0
Canada Customs and Revenue Agency	205	127	31	47	0
Royal Canadian Mounted Police	200	101	71	28	0
National Defence	130	51	58	21	0
Citizenship and Immigration Canada	107	52	49	6	0
Human Resources Development Canada	85	38	16	31	0
Canada Post Corporation	71	37	13	21	0
Justice Canada	65	47	13	5	0
Canadian Security Intelligence Service	57	48	8	1	0
Canadian Nuclear Safety Commission	36	1	0	35	0
Others	230	100	50	80	0
Total	**1,642**	**708**	**542**	**392**	**0**

Top Ten Departments by Complaints Received

April 1, 2002 to March 31, 2003

Organization	Total	Access to Personal Information	Time	Privacy	Other
Correctional Service of Canada	456	106	233	117	0
Canada Customs and Revenue Agency	205	127	31	47	0
Royal Canadian Mounted Police	200	101	71	28	0
National Defence	130	51	58	21	0
Citizenship and Immigration Canada	107	52	49	6	0
Human Resources Development Canada	85	38	16	31	0
Canada Post Corporation	71	37	13	21	0
Justice Canada	65	47	13	5	0
Canadian Security Intelligence Service	57	48	8	1	0
Canadian Nuclear Safety Commission	36	1	0	35	0
Others	230	100	50	80	0
Total	**1,642**	**708**	**542**	**392**	**0**

Completed Investigations and Results by Department

April 1, 2002 to March 31, 2003

Organization	Well-Founded	Well-Founded/Resolved	Not Well-Founded	Discontinued	Resolved	Settled	Total
Agriculture and Agri-Food Canada	2	1	1	2	0	5	**11**
Canada Customs and Revenue Agency	37	14	878	6	8	46	**989**
Canada Mortgage and Housing Corporation	0	0	0	0	0	2	**2**
Canada Post Corporation	17	4	11	6	0	8	**46**
Canadian Heritage	0	0	1	0	0	0	**1**
Canadian Human Rights Commission	0	0	1	0	0	0	**1**
Canadian International Development Agency	1	0	1	0	0	0	**2**
Canadian Nuclear Safety Commission	0	0	35	1	0	0	**36**
Canadian Security Intelligence Service	5	2	18	0	1	0	**26**
Canadian Space Agency	2	0	0	0	0	0	**2**
Citizenship and Immigration Canada	33	4	28	13	0	28	**106**
Commission for Public Complaints against the RCMP	0	0	5	0	0	0	**5**

Completed Investigations and Results by Department (continued)

April 1, 2002 to March 31, 2003

Organization	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discon-tinued	Resolved	Settled	Total
Correctional Service of Canada	189	17	42	11	1	65	325
Environment Canada	0	1	2	3	0	0	6
Farm Credit Corporation Canada	1	0	0	0	0	1	2
Finance Canada	0	1	0	0	0	0	1
Fisheries and Oceans Canada	1	3	4	1	0	0	9
Foreign Affairs and International Trade Canada	0	0	5	0	0	0	5
Freshwater Fish Marketing Corporation	0	1	0	0	0	0	1
Health Canada	2	1	6	1	0	1	11
Human Resources Development Canada	19	7	1,568	6	2	6	1,608
Immigration and Refugee Board	4	4	13	0	0	1	22
Indian and Northern Affairs Canada	1	0	2	0	0	3	6
Industry Canada	0	0	1	0	0	1	2
Inspector General of the CSIS	0	0	2	0	0	0	2
Justice Canada	4	1	11	1	0	7	24
National Archives of Canada	1	0	1	1	0	3	6

Completed Investigations and Results by Department (continued)

April 1, 2002 to March 31, 2003

Organization	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discon-tinued	Resolved	Settled	Total
National Defence	25	7	10	7	1	14	64
National Parole Board	0	0	1	1	0	3	5
Office of the Chief Electoral Officer	0	0	0	1	0	0	1
Office of the Commissioner of Official Languages	0	1	0	0	0	1	2
Privy Council Office	0	1	5	0	0	0	6
Public Service Commission of Canada	1	0	2	0	0	1	4
Public Works and Government Services Canada	3	0	0	0	0	3	6
Royal Canadian Mounted Police	20	5	41	12	0	28	106
Solicitor General Canada	0	0	6	0	0	0	6
Statistics Canada	0	0	6	0	0	6	12
Transport Canada	1	2	0	2	0	1	6
Treasury Board of Canada Secretariat	0	0	2	0	0	0	2
Vancouver Port Authority	0	0	0	1	0	0	1
Veterans Affairs Canada	2	0	2	0	0	1	5
Total	**371**	**77**	**2,711**	**76**	**13**	**235**	**3,483**

Completed Investigations by Grounds and Results

April 1, 2002 to March 31, 2003

	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discon-tinued	Resolved	Settled	Total
Access to Personal Information	14	72	228	36	5	131	**486**
Access	14	71	221	33	5	129	**473**
Correction/ Notation	0	1	7	3	0	0	**11**
Language	0	0	0	0	0	2	**2**
Inappropriate Fees	0	0	0	0	0	0	**0**
Privacy	56	4	2,445	17	8	86	**2,616**
Collection	7	2	831	2	7	19	**868**
Retention and Disposal	4	0	4	0	0	13	**21**
Use and Disclosure	45	2	1,610	15	1	54	**1,727**
Time Limits	301	1	38	23	0	18	**381**
Correction/Time	2	0	0	0	0	0	**2**
Time Limits	287	1	29	23	0	18	**358**
Extension Notice	12	0	9	0	0	0	**21**
Other	0	0	0	0	0	0	**0**
Total	**371**	**77**	**2,711**	**76**	**13**	**235**	**3,483**

Origin of Completed Investigations

April 1, 2002 to March 31, 2003

Province/Territory	Number
Newfoundland	14
Prince Edward Island	3
Nova Scotia	59
New Brunswick	52
Quebec	2,247
National Capital Region–Quebec	22
National Capital Region–Ontario	96
Ontario	396
Manitoba	83
Saskatchewan	55
Alberta	167
British Columbia	273
Nunavut	0
Northwest Territories	0
Yukon	4
International	12
Total	**3,483**

Inquiries under the *Privacy Act*

April 1, 2002 to March 31, 2003: 5,183

We will attempt to provide a breakdown of these inquiries by subject in future Annual Reports.

Origin of Completed Investigations

April 1, 2002 to March 31, 2003

Province/Territory	Number
Newfoundland	14
Prince Edward Island	3
Nova Scotia	59
New Brunswick	52
Quebec	2,247
National Capital Region–Quebec	22
National Capital Region–Ontario	96
Ontario	396
Manitoba	83
Saskatchewan	55
Alberta	167
British Columbia	273
Nunavut	0
Northwest Territories	0
Yukon	4
International	12
Total	**3,483**

Inquiries under the *Privacy Act*

April 1, 2002 to March 31, 2003: 5,183

We will attempt to provide a breakdown of these inquiries by subject in future Annual Reports.

PRIVACY PRACTICES AND REVIEWS

Section 37 of the *Privacy Act* empowers the Commissioner to initiate compliance reviews of the personal information management policies and practices of federal institutions. This means that, at the Commissioner's discretion, he can audit them to determine whether they adhere to the fair information practices set out in sections 4 to 8 of the *Act*. The Privacy Practices and Reviews (PP&R) Branch may evaluate the compliance of organizations with the requirements of the *Privacy Act*.

In the aftermath of September 11, 2001, a number of federal Government departments and agencies received significant funding increases to allow them to implement changes to combat terrorism and enhance national security. To assess the impact that these anti-terrorism measures are having on individual privacy, the Office initiated reviews of the personal information handling practices at the Royal Canadian Mounted Police, the Canadian Security Intelligence Service and the Communications Security Establishment. The reviews will be completed in the upcoming fiscal year.

A number of programs and activities established by federal Government institutions and agencies provide for the disclosure of personal information about Canadian citizens and residents to departments and agencies of the United States government. During this fiscal year, the Office initiated an examination of agreements, arrangements and memoranda of understanding between Canada and the United States that include provisions for the sharing of personal information. Eighteen departments and agencies were selected for this examination and a review will be completed in the upcoming fiscal year.

In addition to reviewing and auditing, our Office advises federal organizations on compliance issues and the privacy implications of new and existing programs and practices. The Office's PP&R Branch has been involved in numerous consultative efforts with Government departments, including the Treasury Board of Canada Secretariat, Elections Canada, Statistics Canada, Human Resources Development Canada, Indian and Northern Affairs Canada, and Health Canada, to name a few.

These consultations often involve reviewing new information management proposals, such as data-matching initiatives, the creation of databases and information-sharing arrangements with other organizations. It is important to note that the Commissioner's role in such issues is an advisory one. The Commissioner does not in any way provide formal approval for such initiatives, which would compromise his impartiality during subsequent investigations or reviews.

As described in our earlier reports, HRDC developed a review procedure to deal with policy analysis, research and evaluation activities involving the linking of separate databanks. Part of this procedure includes consultation with our Office. During the past year, the Office has analyzed and commented on close to a dozen HRDC submissions, including the Evaluation of HRDC Work Sharing Program, the Evaluation of Labour Market Information Services, and the Canada Student Loan Program Needs Assessment and Loans Disbursement Datasets Project.

One project that the department sent our Office, the Employer and Industry Activity System, was submitted as an undertaking involving databank connections. Upon review, our Office concluded that the project involved more than simply the linking of existing databanks. Rather, it would result in the creation of a new databank that would be used on an ongoing basis. It was never contemplated that this type of project would be dealt with through this process. As a result, we advised HRDC that the matter would be more appropriately dealt with by way of a Privacy Impact Assessment (PIA), which entails a more rigorous review. PIAs are discussed in more detail in the following section of this Report.

We have continued to notice an improvement in the detail and completeness with which HRDC's submissions address privacy issues. In our last Report, we expressed a concern that HRDC provided limited information regarding contracts with outside parties, and we said that HRDC should strengthen the contractual obligation of those parties to protect the privacy of personal information under their temporary stewardship. Although some of the submissions we received did not fully meet expectations, the department has improved in addressing this concern over the past year.

PRIVACY IMPACT ASSESSMENTS

On May 2, 2002, the Secretariat of the Treasury Board of Canada issued a new directive requiring federal Government departments and agencies to undertake a Privacy Impact Assessment (PIA) for all new programs or services that raise privacy issues. Canada is the first country in the world to make PIAs mandatory for all federal departments and agencies.

For more than a year prior to that date, the Office had been urging the Government to put a PIA Policy in place, in order to ensure that privacy considerations are built in at the outset of projects and not as an afterthought. In developing this Policy, we congratulate the Government for implementing the Policy and for recognizing that respect for citizens' privacy is critical to the success of all its programs and services, including the Government On-Line initiative.

New and existing programs and services with potential privacy risks must now undergo a PIA – in effect, a feasibility study from a privacy perspective. This includes significant redesigns of existing programs when the redesign involves a new or increased collection, use or disclosure of personal information, new data-matching, contracting-out or other changes that potentially raise new privacy concerns.

A PIA is designed to provide federal Government departments and agencies with a consistent framework to forecast a proposal's impacts on privacy, assess its compliance with privacy legislation and principles, and determine what mitigating measures are required to overcome the negative impacts. If done correctly, a PIA is a way to avoid extra costs, adverse publicity, and the loss of credibility and public confidence that could result from a proposal that is not privacy friendly. It is also a way to raise awareness and understanding of privacy principles, both internally and among citizens.

The conduct of a PIA is a shared responsibility. As the Treasury Board Policy states, PIAs are co-operative endeavours, requiring a variety of skill sets, including those of program managers, technical specialists, and privacy and

legal advisors. Although the deputy head of a federal institution, department, or agency is responsible for determining if a PIA is required, several Government departments have set up internal committees to review departmental projects to determine whether a PIA is required. Given the multi-disciplinary nature of the exercise, this strikes us as a sensible approach.

Of particular significance is the fact that the Policy requires departments to inform the Office of all proposals for new or modified programs and services that raise privacy issues. Departments must also consult the Office while preparing a PIA to ensure that privacy risks are identified and that mitigating actions to deal with those risks are appropriate. By reviewing the documentation in co-operation with institutional officials, our Office is then able to provide advice and guidance to institutions and identify solutions to potential privacy risks.

The Commissioner's role is not to approve or reject projects that are assessed in the PIAs, but rather to assess whether or not departments have done a good job of evaluating the privacy impact of a project or proposal.

To take on this new responsibility, we created a new division within the PP&R Branch devoted entirely to analyzing and providing comments on PIAs submitted for review.

During the period of this Report, our Office received 17 PIAs and 12 preliminary PIAs (PPIAs), and has been consulted on several projects that would require PIAs. Based on discussions with the Treasury Board Secretariat (TBS) and other federal Government departments and agencies, we expect to receive more than 50 PIAs over the next fiscal year.

Most of these initiatives or projects involve the electronic delivery of services to individuals through the Internet, so the privacy risks come from a variety of sources, including systems characteristics, technical infrastructure and design of the on-line service or program.

Five of the 17 PIAs we received were prepared prior to the TBS Policy being introduced, and thus did not adhere to the policy requirements or the guide-

lines associated with the Policy. As a consequence, most were either returned to or withdrawn by the submitting departments to be revised in accordance with the Policy. So far, eight PIAs received have run the full course of the review process.

The Commissioner's role is not to approve or reject projects that are assessed in the PIAs, but rather to assess whether or not departments have done a good job of evaluating the privacy impact of a project or proposal.

While the majority of reports received to date from departments are PIAs, we have witnessed over the course of the year a growing number of Preliminary Privacy Impact Assessments (PPIAs). We believe this trend reflects an inclination on the part of departments to adopt a more cautious and phased approach to the development of their PIAs, given their unfamiliarity with the process and the probable lack of in-house expertise in this area. Where departments are facing a fixed and impending deadline for implementation, we have been advising those departments to directly draft their PIA to expedite the review process.

So far there has been no PIA, and certainly no PPIA, where our staff has not found it necessary to go back to the submitting department for additional information. Some commonly omitted elements include:

- a project implementation schedule;
- a complete inventory of data elements collected and used (information may be described, but not itemized);
- an adequate description of the business process;
- a data flow chart, or one that is complete; and
- an adequate description of the information security infrastructure associated with the project.

In addition to this, background documents commonly missing include:

- draft agreements, where third party service providers are involved;
- Threat and Risk Assessment (TRA) reports, where conducted;
- project feasibility studies, where conducted;
- project management plans, as they relate to project design; and
- technical specifications relating to system design.

There are also a number of common problems which we have observed in the privacy analysis. They include:

- confusing privacy with security and confidentiality;
- seeing the PIA process as essentially a privacy compliance audit exercise;
- failure to link identified risks with specific design elements of the project;
- proposed mitigating measures not addressing the risk identified; and
- proposed mitigating measures for risks that have not yet been identified.

Although these problems and omissions reflect the unfamiliarity of departments with the PIA Policy, it should be noted that we are now beginning to see a general improvement in the quality of the PIAs we are receiving.

If there are lessons to be drawn from our experience of the last eleven months, one is the need for greater education on how the PIA functions as a risk management tool. Another is the need for departments to notify and involve the Office at the earliest possible stage in the development of the PIA.

Given that there is a need for organizations to have a better understanding of the PIA Policy, we advise Government officials to contact the Treasury Board Secretariat or to visit its Web site at **www.tbs-sct.gc.ca** for more information.

IN THE COURTS

Section 41 of the *Privacy Act* allows an individual, following the results of an investigation of a complaint by the Privacy Commissioner, to apply to the Federal Court for review of the decision of a Government institution to refuse the individual access to her personal information. From the time the *Privacy Act* came into force in 1983 to March 31, 2003, approximately 130 applications for review have been filed in the Federal Court. Eight of these were filed in the year ending March 31, 2003.

Section 42 of the *Privacy Act* allows the Commissioner to appear in Federal Court. The Commissioner can apply to the Federal Court for review of the decision of a Government institution to refuse access to personal information if he has the consent of the individual who requested the information. The Commissioner can appear before the court on behalf of an individual who has applied for review under section 41. Or, with leave of the court, he can appear as a party to any review applied for under section 41.

There are currently no applications under the *Privacy Act* in which the Commissioner is actively involved. However, the Commissioner also participates in litigation that arises outside of the *Privacy Act*. Following is a summary of litigation involving significant privacy issues in which the Commissioner has been involved.

Mertie Anne Beatty et al. v. The Chief Statistician et al.

Federal Court File No. T-178-02

This issue was brought before the Federal Court of Canada by a group of Canadian citizens seeking access to the 1906 Census Returns for the Provinces of Manitoba, Saskatchewan and Alberta pursuant to section 6 of the Privacy Regulations.

The Offices's position has always been that disclosure of the 1906 census information is prohibited by the confidentiality provisions in the *Statistics Act*, and that legislative amendments should, therefore, be explored as a means of compromise.

Status

The Application was filed in February 2002. Following a review of the legislation, the federal Government decided that the information could, in fact, be released and did so. Bill S-13 was later introduced in order to retroactively modify census laws to allow access to records and address privacy concerns. Accordingly, the Application was discontinued.

Canada Post Corporation v. Privacy Commissioner of Canada

Federal Court File No. T-233-02

On January 14, 2002, the former Commissioner determined that Canada Post's use of its National Change of Address (NCOA) service contravened the *Privacy Act* in two ways. First, Canada Post contravened section 5(2) of the *Act* by failing to specify to NCOA applicants its intention to disclose new addresses to mass mailers and direct marketers for a commercial purpose. Then it contravened section 8 by failing to obtain the consent of individuals for the disclosure of their new addresses to mass mailers and direct marketers.

Status

On February 13, 2002 Canada Post filed an Application alleging that the former Commissioner had exceeded his jurisdiction in applying sections 5 and 8 of the *Privacy Act*. On April 4, 2002, however, Canada Post agreed to add a box on its form enabling individuals to provide consent for this activity. The issue thus became moot, and Canada Post discontinued its Application on April 14, 2002.

Privacy Commissioner of Canada v. Attorney General (Canada) et al.

British Columbia Supreme Court File No. S57566

In June 2001 the Office received a complaint regarding the installation of Royal Canadian Mounted Police (RCMP) surveillance cameras in the downtown core of the City of Kelowna, B.C. After an investigation, the former Commissioner determined that by recording continuously rather than recording only selective incidents related to law enforcement activities, the

RCMP is unnecessarily collecting information on thousands of innocent citizens engaged in activities irrelevant to the mandate of the RCMP. It was concluded, therefore, that the video surveillance in Kelowna was in contravention of the *Privacy Act*.

The RCMP informed this Office that the continuous video recording of the surveillance camera was terminated on August 28, 2001. Instead, the area under surveillance would only be videotaped if a violation of the law was detected. While this put the use of the surveillance camera into compliance with the letter of the *Privacy Act*, which technically only applies to information that is "recorded in any form", it was the former Commissioner's opinion that a continuation of the video camera surveillance even without continuous recording was insufficiently respectful of the spirit of the *Privacy Act* and of the privacy rights of Canadians.

On June 21, 2002, the former Commissioner filed a Statement of Claim in the Supreme Court of British Columbia, requesting declarations from the Court that this generalized video surveillance was unconstitutional, contravening the *Charter*, as well as Canada's international human rights obligations. From March 12 to 14, 2003 there was a hearing on the federal Government's motion to dismiss the case. The court held that the Commissioner lacked the legal capacity to bring the action.

Status

On July 4, 2003, the newly-appointed Commissioner announced that he had instructed counsel to withdraw its appeal into the case. Although the Commissioner and this Office continue to have a variety of concerns regarding video surveillance of public places by public authorities, continuing this particular action was not perceived as a useful way of spending public funds.

Information Commissioner of Canada v. Commissioner of the RCMP et al.

Supreme Court of Canada File No. 28601

A list of the career postings of four Royal Canada Mounted Police (RCMP) officers was requested under the *Access to Information Act*. The Commissioner of the RCMP refused to release the information on the grounds that it revealed employment history and thus was personal information as defined in section 3 of the *Privacy Act*. The Information Commissioner argued, however, that paragraph 3(j) of the definition of personal information in the *Privacy Act* states that information relating to the position or functions of Government officers or employees is not personal information for the purposes of section 19 of the *Access to Information Act*.

Status

The Supreme Court of Canada released their unanimous decision on March 6, 2003. The Court very clearly stated that information may be personal and yet still fall under the rubric of section 3(j) where it reveals general characteristics associated with the position or functions held by an officer or employee of a federal institution. The Supreme Court felt that none of the information requested pertained to the competence or characteristics of the employees. It therefore ordered that the following information be released for each of the named individuals: a list of historical postings, status and dates, a list of ranks and dates those ranks were achieved, and the years of service and anniversary date of service.

The decision of the Supreme Court limits the application of paragraph 3(j) of the definition. Even though this Office had argued for a narrower interpretation of the exception, the decision of the Supreme Court is not unreasonable.

Part Two

Report on the *Personal Information Protection and Electronic Documents Act*

INTRODUCTION

The *Personal Information Protection and Electronic Documents (PIPED) Act* sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

Since the *Act* took effect on January 1, 2001 it has applied mainly to the commercial activities of what are known as federal works, undertakings or businesses, such as transportation and telecommunications companies, banks and broadcasters. It also applies to the personal information of employees in those companies, and it applies to personal information that is sold, leased, or bartered across provincial or national boundaries by provincially-regulated organizations. As of January 1, 2002, the personal health information collected, used or disclosed by these organizations is also covered. On January 1, 2004, the *PIPED Act* will cover the collection, use or disclosure of personal information in the course of all commercial activities in Canada, except in provinces which have enacted legislation that is deemed to be substantially similar to the federal law.

The second full year under the *PIPED Act* proved to be an interesting and challenging one for our Office on several fronts. We began to accept and investigate complaints that concern the personal health information of individuals. We also made further inroads into a myriad of issues, including consent and marketing, credit scoring, the recording of telephone calls and security clearances.

We also undertook a number of communications activities to raise awareness of privacy issues and federal privacy laws. From April 1, 2002 to March 31, 2003 the former Commissioner and senior staff delivered 49 speeches at conferences and special events; we issued more than 25 news releases and media advisories on key privacy issues; we responded to hundreds of media requests for information and interviews; we disseminated more than 23,000 of our publications to members of the public, businesses and other organizations across the country; and we received an ever-increasing number of hits to the Web site, averaging approximately 50,000 hits per month.

The *PIPED Act* requires the Commissioner to submit an Annual Report to Parliament on the activities of the Office in the previous year. The current Report covers the period from January 1, 2002 to December 31, 2002 for the *PIPED Act*.

INVESTIGATIONS AND INQUIRIES

During the 2002 calendar year, the Office received 300 complaints under the *PIPED Act* from individuals alleging that their privacy rights had been violated by a wide range of different organizations. Approximately 37% of the cases dealt with practices in the banking sector, followed by 19% with the telecommunications and broadcasting sector, 15% with transportation companies, and 13% with the nuclear sector. The remaining complaints, 16%, were filed against a variety of other types of organizations, including Internet service providers, credit bureaus and aboriginal band councils.

The former Commissioner issued findings for 162 complaints under the *PIPED Act* in 2002 and they were concluded as follows:

Not well-founded	61
Well-founded	45
Resolved	41
Discontinued	15

In addition to this, the Office also conducted five incident investigations. Incidents are matters that the Commissioner becomes aware of from various sources, including the media. Usually a victim is not identified and a complaint has not been filed with the Office.

What follows in this Report is a sampling of some of the year's more notable cases. More detailed summaries of all findings under the *PIPED Act* are available on our Web site, at **www.privcom.gc.ca**. These findings are posted in order to provide guidance to organizations and the legal community on the application of the *Act*.

DEFINITIONS OF FINDINGS UNDER THE *PIPED ACT*

Not well-founded: This means that there is no evidence to lead the Privacy Commissioner to conclude that the organization violated the *Personal Information Protection and Electronic Documents (PIPED) Act*.

Well-founded: This means that the investigation revealed that the organization failed to respect a provision of the *Personal Information Protection and Electronic Documents (PIPED) Act*.

Resolved: This means that the organization has taken corrective action to remedy the situation, or that the complainant is satisfied with the results of the inquiries made by the Office of the Privacy Commissioner of Canada.

Discontinued: This category applies to investigations that are terminated before all the allegations have been fully investigated. A case may be discontinued for any number of reasons, such as the complainant no longer being interested in pursuing the matter.

SUMMARY OF SELECT CASES UNDER THE *PIPED ACT*

A case of mistaken identity

A complainant who wrote to the Office said she was notified by a friend that a notice in the newspaper indicated that the police were looking for her. To her horror, the complainant found herself looking at her own image in a photograph accompanying the Crime Stoppers "Crime of the Week" article. The article described a recent theft of two cheques from an elderly woman and identified the depicted person as a suspect in the crime. The image had been captured from a video surveillance camera at a bank. The camera had been pointed at the teller's wicket where the thief had cashed the stolen cheques.

As it turned out, the complainant had indeed visited the same bank and the same teller's wicket on the day in question, but not to cash a cheque. She had gone there simply to pay a bill. It was clear that she was not the actual perpetrator of the crime.

It was the same bank, the same wicket, the same day, but not, as our investigator learned, the same time.

On the day in question, the clock on the bank's journal roll (its computerized record of transactions) had been 12 minutes slower than the clock on the video camera. When the bank's security staff later forwarded the videotape to the time of the cheque-cashing as indicated by the journal roll, the image that appeared was not that of the actual cheque-casher. Rather, it was the image of the woman who had preceded the cheque-casher at the teller's wicket by some 12 minutes – the complainant.

Thus, the photographs that the bank subsequently gave to the local police, and the police in turn to the Crime Stoppers organization, depicted the wrong person.

To her horror, the complainant found herself looking at her own image in a photograph accompanying the Crime Stoppers "Crime of the Week" article.

A week after the original "Crime of the Week" article, Crime Stoppers ran a retraction in the same local newspaper. On the same day, the newspaper itself ran a front-page story, clarifying that the complainant had been a victim of mistaken identity. The complainant also received formal apologies from the bank, the police, and Crime Stoppers. The two latter organizations further admitted that they had both failed to follow normal verification procedures, and both have since collaborated in instituting measures to prevent similar occurrences. The bank also instituted procedural changes to verify the time on surveillance tapes and journal rolls.

However, the complainant was not entirely satisfied. After her initial shock and distress, she became even more concerned about the effect the incident was having on her reputation when she learned that many people had indeed recognized her image from the article. This was of particular concern because her work depended upon her ability to visit clients' homes and offices. She was also concerned that her image may have appeared in other Crime Stoppers notices. Our Office was able to reassure the complainant that her photograph had been used in only the one newspaper article.

As to the disposition of her formal complaint to the former Commissioner, we considered the matter in relation to the bank's obligations under the *PIPED Act* to ensure the accuracy of personal information.

We determined that the personal information at issue – the photograph of the complainant – had been wholly inaccurate in a situation where accuracy had been crucial to the purpose of solving a crime. On that account alone, the bank should have made sure that the information it disclosed was as accurate as possible. It had not done so, and therefore was in clear contravention of Principle 4.6 of the *Act*. In the letter of findings to the complainant, the former Commissioner wrote:

> *" ... an organization must take due account of the potential adverse consequences of inaccurate information for the individual. I have determined that your personal information inaccurately disclosed by [the bank] was used to make a decision about you – specifically, an erroneous decision to the effect you were to be sought as a prime suspect in a crime. This was a decision, moreover, that caused you substantial notoriety, embarrassment, and worry about your reputation and your livelihood. Being well aware that the police would likely use your personal information to make a decision about your status as a suspect, the [bank] should have taken due care to ensure that the information was accurate so as to minimize the possibility of a wrong decision with adverse consequences for you."*

The former Commissioner determined that this complaint was well-founded.

U.S. security measures affect Canadian pilots

The aftermath of September 11, 2001 continues to be felt by average Canadians. One individual directly affected by new security measures, a commercial airline pilot, was confronted with a difficult choice: forfeit his privacy rights or risk losing his job. In the past, when he needed to take aircraft training required to keep his licence, his employer simply sent him to a flight school in Florida. This changed after the September 11 terrorist attacks. American flight schools were now obliged to have their foreign students – including Canadian commercial airline pilots – sign an authorization form. The form would allow the U.S. government to collect and disclose personal information about the students. However, it did not adequately explain the purposes for, nor did it appear to set any limits on, this collection and disclosure.

When his employer asked him to sign the form, the pilot was incensed. After all, he had already undergone an extensive background check by the Government of Canada. He disliked the prospect of a foreign government sifting through his background – especially when it was not clear what information would be collected and to whom it would be disclosed.

He disliked the prospect of a foreign government sifting through his background – especially when it was not clear what information would be collected and to whom it would be disclosed.

No one seemed comfortable with the form – the Canadian Government, the airline, the union – but there was no immediate solution on the horizon. The federal Government had asked the United States to accept Canadian background checks on commercial pilots. But at the time of the complaint, the United States had not yet made a decision.

The airline was troubled by the wording of the form, but was in a difficult situation. By law, its pilots require the training. The nearest alternative was a flight school in Europe – a more costly prospect than sending its pilots to Florida. Furthermore, since the pilot and co-pilot must train together, the airline would be in an awkward position if one pilot was willing to sign the form and the other was not.

The pilot's union protested the requirement to sign the form. It negotiated an agreement with the airline which stated, among other things, that the decision to sign the form was voluntary, and that the company would provide alternative training for dissenting pilots.

The pilot decided not to sign the form. Although his employer obtained a temporary extension of his licence until a resolution could be found, it did

not make alternative training arrangements for him. Unless the U.S. government agreed to Canada's request, or the former Privacy Commissioner made his findings, the airline was not going to change its decision. The pilot's extension eventually ran out.

We were highly critical of the authorization form. It was entirely objectionable on many fronts and we concluded that the practices it authorized completely failed to meet the fair information principles that are the cornerstone of Canada's privacy legislation.

In making these determinations, we relied on the "reasonable person test" outlined in section 5(3) of the *PIPED Act* to assess the airline's purposes. We acknowledged that, on the surface, the airline's reasons for making its pilots sign this form appeared reasonable. Below the surface, however, the purposes ceased to be acceptable. We thought very little of the airline putting cost and convenience ahead of the pilot's right to refuse consent to collection and disclosure practices that were clearly in contravention of Canadian law. It was noted that the airline had options but that it had chosen not to exercise them.

In finding that the airline's purposes did not meet the expectations of section 5(3), in the letter of findings, the former Commissioner commented on this timely example of the difficulty of balancing national security requirements with the fundamental right of privacy:

> *"I agree that the circumstances that many countries, most particularly the United States, currently find themselves in warrant some security measures. Of course it is reasonable to demand that pilots receive security clearance in order to fly, and that is why Canada has in place security measures that Canadian commercial pilots must undergo... But would a reasonable person consider it appropriate to require these same pilots to then consent to unacceptable collection and disclosure practices at the request of a foreign government? I think not. Indeed, I suspect most reasonable Canadians would find this encroachment on Canadian rights to be highly objectionable. Furthermore, most*

Canadians would likely expect employers to provide reasonable options for employees and would demand that their government raise an alarm bell with the United States."

After receiving the letter of findings, the airline agreed with the former Commissioner's recommendation and arranged to provide training at an alternative location for the pilot and others who refuse to sign the form.

Bank's disclosure to individual's employer inappropriate

An individual went to his bank on personal business – to dispute a charge for cheques. He was not satisfied with the bank's response he was given and a scene ensued.

The branch manager came onto the scene and decided his staff should not have to deal any further with the customer. The firm that employed the customer happened to do a lot of important business with the bank. Before terminating the bank's relationship with the customer, the branch manager thought he should discuss the matter with the customer's employer.

The complainant was astounded when his employer confronted him about what had occurred at the bank earlier that morning.

One of our first tasks was to determine what exactly had been disclosed in the telephone conversation between the bank manager and the employer. In the absence of any evidence that they had discussed the complainant's financial affairs, it appeared that the actual disclosures about had been limited to three simple facts: (1) that he had an account with the branch; (2) that his account was to be terminated; and (3) that there had been a scene with the teller.

In the bank's view, none of this should have been considered the complainant's personal information. The bank pointed out that the scene itself had been acted out in a public place, and in a small community, where a person does his banking is hardly a matter of secrecy. The bank took the position that the disclosures in question fell into the category of "normal public discourse," comparable to "small-town gossip." The bank even suggested that it

had a right to make such disclosures for the sake of extending "business courtesy" and protecting its own business interests. Citing section 5(3) and Principle 4.3.5, the so-called "reasonableness" provisions of the *PIPED Act*, the bank also suggested that the complainant had not had a reasonable expectation of privacy, and that reasonable people would have considered the disclosures appropriate in the circumstances.

Although we were not unsympathetic to the bank and were willing to concede the reasonableness of the bank's position up to a point, the former Commissioner had to draw the line somewhere. In the letter of findings to the complainant, the former Commissioner commented as follows:

> *"In my view, ... the reasonableness of the situation ends exactly at the point where the [bank] manager, in the full knowledge that you had been acting on your own behalf at his branch that morning, nevertheless picked up the telephone at his office during business hours to inform your employer. This was not casual or inadvertent disclosure. This was not small-town gossip. This was a deliberate act of disclosure of personal information to a third party by a person who was acting in an official capacity and who had no right to make such disclosure. Moreover, the Act puts the rights of individuals above such notions as 'business courtesy' and makes no distinction as to the size of one's community. Would any reasonable person anywhere expect his bank manager to disclose information about his personal banking affairs to his employer? The answer to this question is obviously no."*

Credit score fraud

In the course of investigating complaints about credit reporting and scoring, we learned a great deal about the workings of the credit-granting industry at large.

In two particular cases, individuals had made formal requests under the *PIPED Act* for access to certain personal information on file with their banks. Specifically, each requester had wanted to know his credit score. The banks in question had refused access, each invoking the exemption provided in section 9(3)(b) of the *Act*. This provision says in effect that an organization does not

have to give access to personal information if doing so "would reveal confidential commercial information."

In the course of investigating complaints about credit reporting and scoring, we learned a great deal about the workings of the credit-granting industry at large.

The requesters, believing to the contrary that credit scores were personal information to which they were fully entitled to have access, filed complaints with the Office. Our main task in each case was to decide whether the exemption cited by the bank was valid.

A credit score is a numerical indication of credit-worthiness, generated by means of an algorithmic model. For most people familiar with the notion, the term "credit score" mainly conjures up the vision of credit-reporting agencies. These agencies are in the business of providing banks and other credit-granting institutions with background credit information, sometimes including credit scores, on prospective clients. In considering an application for credit, a credit-granting institution will often obtain the applicant's credit history from a credit-reporting agency. In some cases, the institution will also request a credit score for the applicant. Credit-reporting agencies do not themselves generate credit scores, but rather provide scores that another company generates from the agency's information.

Up to a point, the complainants had good grounds for their position. In prior cases, we had already considered the matter of access to personal credit information, at least as far as credit reporting agencies were concerned. We had already concluded that credit scores *are* personal information according to the definition in the *Act*, and that individuals *do* in principle have a right of access to them. We had determined that credit-reporting agencies in particular are required to comply with Principle 4.9 of the *Act* by giving individuals access on request to personal information in their credit files. We had fur-

ther determined that banks, if they have obtained an individual's credit information from a credit-reporting agency, must likewise give the individual access on request to the information, including any credit score provided by the agency.

But the more recent cases were not nearly as straightforward. The special problem they presented was that the credit scores sought by the complainants were not the usual agency-provided credit scores. They were in fact scores that the banks themselves had generated and assigned internally.

It is perhaps less widely known that banks, too, have credit scores, distinct from those provided by credit-reporting agencies. Banks generate their own internal credit scores by means of their own internal credit-scoring models, very different from those associated with agencies. Whereas agency scores are generated by means of standardized models based almost exclusively on credit information, a bank develops its own customized models, unique to the bank and incorporating not only credit information on the individual, but also many other elements pertaining to the bank's own strategic business priorities. Because banks regard and treat their internal credit-scoring models as proprietary confidential commercial information, such models are much more problematic in terms of the *Act*.

By citing section 9(3)(b), the banks in question were not suggesting that an internally generated credit score was itself confidential commercial information. Rather, they were saying that the model used to generate such a score was confidential commercial information. And they were saying in effect that internal credit scores, if made available to individuals, would reveal the model by which the scores had been generated.

The special problem they presented was that the credit scores sought by the complainants were not the usual agency-provided credit scores.

We accepted the banks' arguments that an internal credit-scoring model constituted confidential commercial information. But we were far less persuaded of the more crucial proposition – that releasing the credit scores would somehow reveal the credit-scoring model itself. How could merely letting a person know his credit score possibly lead to his knowing the inner workings of such a complicated, technical and algorithmic apparatus as a credit-scoring model?

As it turned out, it was not the average customer that the banks feared. It was fraudsters intent on "cracking" a bank's internal credit-scoring model for nefarious purposes. According to the banks, fraudsters could employ devious means to acquire a number of credit scores and then would extrapolate the model from the scores. Either the fraudsters would be working for the banks' credit competitors, trying to gain competitive advantage. Or they would be operating on their own behalf, trying to procure credit for themselves on false pretenses.

In their submissions to the Office, the banks presented an independent forensic analysis of the risk of fraud contingent upon the availability of credit scores. This analysis concluded that, if credit scores were readily available, the integrity of a bank's internal credit-scoring model could be compromised on the basis of a relatively small number of credit scores generated by the model.

The fraud scenarios outlined by the banks struck us as farfetched. To be fair, however, we sought the advice of an expert in the field of algorithms. This expert confirmed that access to customized credit scores would definitely make it easier to approximate a bank's internal credit-scoring model.

We were still doubtful. In particular, we were mindful that section 9(3)(b), by using the phrase "would reveal" rather than "could reveal", set a very high standard for the withholding of personal information. On the word of the algorithm expert, we were willing to concede that a model could be approximated from knowledge of a certain number of scores, but we remained unpersuaded that it would ever happen. The banks' submissions had failed to convince us that fraudsters would actually go the lengths described to deceive a bank. We found it particularly difficult to accept the apprehension, evidently

shared by all banks, that even one's competitors in the credit-granting community would as a matter of course resort to such tactics in order to "crack" one another's models for the sake of competitive advantage.

Nevertheless, the fact remained that two banks had strongly expressed what we took to be genuine belief and fear that their internal credit-scoring models would inevitably be revealed and fraudulently manipulated if individuals were given access to credit scores. However unlikely it seemed to us, it was undeniably a prospect that the banks took very seriously. Moreover, it was a prospect that we were unable to wholly refute.

In the end, the former Commissioner decided to give the banks the benefit of the doubt. He did so primarily out of consideration for his responsibility to achieve a balance between the privacy rights of individuals and the legitimate informational interests of organizations. Seeing little informative value in a credit score on its own and no significant harm ensuing to Canadians' privacy rights from the inability to obtain internal credit scores, we thought it only fair in the circumstances to accept the banks' position.

The former Commissioner found that the banks had appropriately cited section 9(3)(b) to refuse the complainants access to their internal credit scores.

Customers beware: Your conversation may be recorded

The practice of taping customer telephone calls – common among many organizations – was the subject of two complaints. These cases illustrate two very different approaches taken by organizations to inform customers of the practice and obtain their consent. In both cases, as in those involving secondary marketing, reasonable expectations played a role in the former Commissioner's findings.

In the first case, an individual called his bank in the intended role of guarantor of his daughter's loan application. At the end of the conversation, he learned that his call had been tape-recorded. He had not been informed, either by the customer service representative or via a recorded message, that

his call would be taped. Nor was he asked, upon learning that the call had been recorded, if he agreed.

The bank had an interesting take on the issue of consent in this case. In its view, only one party had to consent to calls being recorded. It therefore required its customer service agents to sign a consent form for the taping of these calls.

The bank's purpose for recording the call was that it needed confirmation of the customer's records and evidence that the customer had consented to the product or service. In its view, the taped call is the equivalent of a signed form and is used for record-keeping purposes.

We agree that information exchanged during the conversation should be recorded in some way. However, the reasonable expectations of the customer should also be considered, and most individuals would want to know *beforehand* that their call is going to or may be taped. In this case, the bank clearly did not meet those expectations and did not have the father's consent to record his call, thus contravening the consent principle of the *PIPED Act*.

In the other complaint, an individual also alleged that his bank had recorded his telephone conversations without his knowledge and consent. This individual had taken the bank to court over liability for certain withdrawals made on his bankcard. During this process, the bank introduced a tape-recording of a telephone conversation between him and a bank employee.

The bank argued that it had this individual's consent to tape his calls. It referred to an agreement, signed by him when he opened his account, that acknowledged the bank's practice of recording telephone calls. There were also the privacy brochures given to him – five in all – which specified

...most individuals would want to know beforehand that their call is going to or may be taped.

the bank's purposes for collecting personal information. The complainant, however, did not read any of this information.

Then, there was a conversation between a bank employee and the complainant (also taped), in which the employee explained the bank's practice of recording conversations. To the complainant, "recording" did not necessarily mean electronic recording, and so he stood by his original complaint.

The former Commissioner determined that the bank had made a reasonable effort to inform the complainant of its practice and purpose and that it had his consent to record his calls by way of the agreement form that he had signed. We then found that the bank had complied with the relevant provisions of the *Act*.

Clearly, organizations such as this one, which have made the effort to inform customers and to obtain their consent, have the reasonable expectation that customers will read what is put in front of them.

Nevertheless, the bank in the second case was keen on improving its practices regarding the taping of telephone calls. In response, the Office developed a "best practices" guideline for recording customer telephone calls. Essentially, the guideline states that the taping of telephone calls involves the collection of personal information – a practice that should meet fair information principles. In other words, conversations should not be taped unless it is for a purpose that a reasonable person would consider appropriate in the circumstances. The customer must be informed of the purpose for taping the call and must consent, except in certain limited cases where consent is not required, before the taping begins. The customer should also be offered an alternative, such as not taping the call, visiting a retail outlet, writing a letter, or conducting the transaction over the Internet.

A tape recording captures more than just the specifics needed for the purpose of the call. It records comments, accents and attitudes – information that may not be relevant to the material required. For these reasons, it is important for organizations to be open with customers – to advise them that they record,

explain why they record, and offer them options if they do not want to be recorded.

In both complaints, we provided the banks with our "best practices" guideline and both organizations undertook improvements to their recording practices. In the first case, the bank now notifies customers at the beginning of a call that the conversation is being taped and provides them with alternative means of communicating their information should they not wish to proceed with the call. In the second case, the bank introduced a recorded message to inform all callers that conversations would be tape-recorded.

ISP holds e-mails "hostage"

A customer had complained when she learned that her Internet service provider (ISP) was continuing to receive and store her incoming e-mails while her account was suspended. This is in fact standard industry practice. Many ISPs use continued receipt and storage of e-mails as leverage in collecting on overdue payments.

In this case, the former Commissioner determined that the ISP had not properly informed the complainant of purposes related to the use of her personal information during an account suspension and had thus used her personal information without her informed consent for purposes other than those for which the information had been collected. On this basis, we concluded that the complaint was well-founded.

But this case left the Office highly concerned about the practice at issue, which we knew to be widespread in the industry. In the letters of findings, the former Commissioner commented as follows:

> *"... As Privacy Commissioner, I am concerned about the implications of storing and withholding potentially important messages without informing the intended recipient of their existence or the sender of their non-delivery. As an occasional sender of e-mails myself, rather than be falsely led to believe that a certain message had gone through unimpeded, I would much prefer to have it*

returned with a notification of non-delivery so that I could try to reach the intended recipient by other means. Indeed, returning the message with a notification strikes me as the most appropriate and responsible course of action for an Internet service provider to take in such circumstances."

To answer the above question, then, what an ISP should do in cases of account suspension is what we recommended as best practices in the case in question, as follows:

- Cease collecting, storing, and denying access to, e-mails addressed to holders of accounts under suspension.
- Adopt instead the practice of deflecting such e-mails back to senders with notification to the effect that the messages could not be delivered.
- Make provision for giving the holder of a suspended account access to any e-mails already received by the company, but still unretrieved by the customer, at the time the suspension took effect.

Make sure to check those Government authorities

An individual's holiday memories were marred when he found out that the airline he had used for his trip released his itinerary to his boss. His employer, a federal Government department, was conducting an investigation into his use of sick leave. It approached the airline and requested confirmation of his travel itinerary.

The airline hesitated. Citing its responsibilities under the *PIPED Act*, it asked the department for proof that the individual had consented to such a disclosure. If that was not possible, the airline suggested that a specific exemption or exception under the *Act* would be needed before it would comply with the request.

In response, the department cited a directive under the authority of a specific federal statute, indicated that the information was needed to administer federal public servants' employment legislation, and asked the airline to disclose the itinerary. Satisfied that the department's request fit the exemption

provided in section 7(3)(c.1)(iii) of the *Act*, the airline duly released the information. This section allows an organization to release information about an individual to a Government institution for the purpose of administering a law.

There was just one problem. The department did not quote the correct directive as its lawful authority. Even though it later acknowledged its mistake, the department maintained that it nevertheless had the authority to collect the information – just under different legislation.

We agreed that the department had lawful authority. We were concerned, however, that the department had initially made an error and that the airline had not verified whether the cited directive was correct or not. Although the airline made the disclosure in good faith, an organization has a duty to be vigilant about checking authorities cited by Government organizations before releasing personal information. In his letter of findings the former Commissioner stated:

> *"...where requests for disclosure of personal information are concerned, I consider it incumbent upon any private-sector organization not to take the submissions of any government institution at face value, but rather to be vigilant about checking authorities cited."*

Fees for access: Should you have to pay for your own information?

Responding to requests for access to personal information may entail some costs for organizations. Should it also entail costs for the individual? In fact, there is a provision in the *Act* that allows organizations to charge a fee in responding to requests. But how much is reasonable? This question was addressed in two cases where the complainants accused organizations of charging excessively high fees.

The complainants were involved in disputes with their respective banks concerning money they had borrowed. Both individuals requested their personal

information. The banks responded by demanding fees of $150 and $200 respectively to cover the costs of processing the documents in question. The first individual wanted to know what he would get for his money and when told what this would be decided to file a complaint. The second individual is on a fixed income and could not afford to pay for his personal information.

These cases are good examples of the private sector adjusting to the expectations of the Act.

These cases are good examples of the private sector adjusting to the expectations of the *Act*. The banks were reminded that Principle 4.9.4 of the *PIPED Act* stipulates that an organization must respond to an individual's request at minimal or no cost to the individual. As a result, one bank released the information free of charge, while the other asked for a nominal fee of $10.

Additionally, the bank's position in the first complaint seemed to be based not only on cost-recovery but also on its desire to have the complainant meet with it to discuss the dispute that had prompted the access request in the first place. We emphasized to the bank, however, that the *Act* does not require an individual to explain why he or she wants access to personal information or require that he or she enter into any discussions with an organization. In other words, personal information cannot be held for ransom.

Based on the findings in these cases, the bottom line for organizations when it comes to fees is this: cost-recovery does not apply to access to information requests.

A security clearance becomes a job requirement

Protecting nuclear sites from terrorist attacks is a grave concern, particularly in the wake of September 11, 2001. The federal agency that oversees the operations of all nuclear facilities in Canada responded to the terrorist threat by instructing its licencees to implement enhanced security measures. One of

the new measures in place is to limit entry to nuclear facilities to persons with the proper security clearance. If a licencee fails to comply, the federal agency will revoke its operating licence.

A company's nuclear products division informed its employees of the new security requirement and asked them to consent to a security clearance check. Along with a consent form, each employee received an information package that specified the type of information to be collected, the purpose, and the organization that would carry out the collection. Employees were also told that the organization collecting the personal information was bound by a confidentiality agreement.

In order to be granted a security clearance, employees with at least ten years of service were required to pass a criminal records check. Employees with less than ten years of service had to pass a full background check that included employment history, professional qualifications, and personal references, as well as a criminal records check.

Some employees were unhappy and complained to the Office. They felt they did not really have a choice – if they refused, they faced job loss. If they consented but failed the security check, they would lose their current positions and be reassigned, possibly to lower paying jobs. Under those circumstances, they felt their consent was coerced.

The former Commissioner had to determine whether the company was collecting personal information with the employees' knowledge and consent as required under Principle 4.3 of the *PIPED Act*. Clearly, the employees knew of the collection. But was their consent voluntary? In the letters of findings, the former Commissioner assessed the issue as follows:

> *"[The company] expressly asked you for your consent, and it is entirely up to you whether to give it or not. That there may be unpleasant consequences in either case does not alter the fact that you do have a choice in the matter. Refusal to give consent to the collection of personal information may very often entail unpleasant consequences for the individual. But in this case, as in most*

decisions in life where the prospect of unpleasant consequences is a factor, the pressure you may feel to consent to the collection does not amount to duress. Under the Act, the key consideration is not whether there may be unpleasant consequences to an individual's refusal to give consent, but rather whether the collection is itself reasonable."

Was it reasonable for personal information to be collected for the purposes of a security clearance as stipulated by section 5(3) of the *Act*? The former Commissioner concluded that it is entirely reasonable for the federal agency to impose an enhanced security requirement upon its licencees, given the greatly enhanced concern about possible acts of terrorism at nuclear facilities. Had the company not complied, it would have lost its licence to produce nuclear fuels and would no longer have been able to conduct its nuclear products business, leading to substantial financial losses and staff lay-offs. Under these circumstances, we determined that it was entirely reasonable for the company to comply with the order and thus collect personal information from employees to conduct security clearance checks.

Aeroplan: Opt-out consent is not enough

When Air Canada mailed out privacy brochures to 60,000 Aeroplan members, several members complained to the Office.

The individuals who complained to the Office did not mind that the company had made the effort to seek their consent to information-sharing practices under the Aeroplan program. What they did object to, however, was having the onus put on *them* to tell Air Canada if they did *not* consent to the practices outlined in the brochure. Nor did they appreciate that the company was presuming, in the meantime, that they did consent.

The former Commissioner concluded that Air Canada was not in compliance with the *PIPED Act* and that the complaints were well-founded.

The 60,000 brochures accounted for only about one per cent of Aeroplan's total membership at the time. In the letters of findings, the former Commissioner

remarked that the *Act* required organizations to observe every individual's privacy rights and did not allow for token compliance. Since Air Canada had in effect left 99% of Aeroplan members in the dark about its information-handling policy and practices, the former Commissioner found its attempt at seeking consent to have been entirely inadequate.

Even if all plan members had been consulted, the brochure itself failed to seek consent in an appropriate form. It described five ways in which Air Canada was intending to share Aeroplan members' personal information under the program. Each description was accompanied by a check-off box, and the plan member was instructed to check the box only if he or she did not consent to having personal information shared in the manner described. Any plan member checking off one or more of the five boxes was then expected to mail the brochure back to the company by way of expressing non-consent. Conversely, any plan member who did not return the brochure was considered to have consented to all five information-sharing situations.

This form of consent has come to be known as "negative" or "opt-out" consent. It correlates to the "negative option" marketing practices that consumers have been so quick to condemn in the past. In effect, such practice is based on presumption – the individual is presumed to agree to a proposition unless he or she takes the initiative to refuse it.

Like most other people involved in the protection of privacy, and indeed like most informed consumers, we hold a very low opinion of the negative option as it is used

Like most other people involved in the protection of privacy, and indeed like most informed consumers, we hold a very low opinion of the negative option as it is used by organizations in their handling of personal information.

by organizations in their handling of personal information. The Office considers opt-out to be a weak form of consent – one that unfairly puts the onus of initiative on the wrong party and reflects at best a mere token observance of what is perhaps the most fundamental principle of the *Act*. We would prefer that organizations adopt an exclusively "positive" or "opt-in" approach – a much more respectful approach whereby individuals would be deemed to have consented only if they have expressed a definite "yes" to a proposition.

On the other hand, the Office is also well aware that opt-out is a form of consent expressly permitted by the *Act* in certain circumstances – notably, where the personal information is of a demonstrably non-sensitive nature. The problem here is that the *Act* itself refrains from precisely defining the notion of sensitivity. Although it does instruct that an individual's financial and medical information is almost always to be considered sensitive, it also goes on to suggest that any information can be sensitive, depending on the context. In the Aeroplan complaints, therefore, the Office's task was essentially one of assessing the context. In other words, the former Commissioner had to determine whether the circumstances justified Air Canada's recourse to opt-out consent.

In the letters of findings, the former Commissioner made a point of stating that the intention is always to keep strict limits upon the circumstances in which opt-out could be deemed appropriate. It was also made clear that the Office intends to be guided in all such deliberations by due consideration for both the sensitivity of the information and the reasonable expectations of the individual. It was on these considerations that the Aeroplan privacy brochure ultimately failed.

The language of the brochure failed to demonstrate that any of the information-sharing situations described was strictly non-sensitive in nature or context. Two of the situations were of a particularly high order of sensitivity. The other three seemed by their descriptions to allow for considerable marketing to individuals on the basis of information customized according to potentially sensitive criteria. As it was put in the former Commissioner's letters:

"Although in my view the practice of sharing plan members' information for purposes of offering special promotions and products remains unobjectionable in itself, I am satisfied that a reasonable person would not expect such practice to extend to the 'tailoring' of information to the individual's potentially sensitive interests, uses, and preferences without the positive consent of the individual."

The former Commissioner concluded that it had been inappropriate for Air Canada to seek negative or opt-out consent to Aeroplan's information-sharing policies and practices as described in the brochure.

To its credit, Air Canada took the Commission's findings and recommendations very seriously. With some guidance from the Office, in a process that we found to be both positive and productive, the company undertook to rethink and rewrite its information-sharing policy under Aeroplan. We have reviewed the finished product, and have verified that the policy now addresses our concerns in the following ways:

- It explains to Aeroplan members, in clear and understandable terms, the purposes for the collection, use, and disclosure of personal information under the program.
- It explains clearly that Aeroplan does not collect any details of the transactions whereby members accumulate points under the program.
- It specifies that Aeroplan does not provide individualized profiles of members to partner companies or other third parties, and further clarifies that any information provided to partners can be used only for purposes related to the Aeroplan program.
- It explicitly and clearly states that members who wish to have their personal information used only for redemption of Aeroplan points can so stipulate, and it identifies an easily-executable procedure for members to exercise this option.

As for the matter of consulting the full Aeroplan membership, Air Canada also set out a very specific plan whereby all active members of the program would

receive a copy of the revised policy with their next account statements. Moreover, the policy was to be made available on the Aeroplan Web site.

We were satisfied that Air Canada had responded appropriately to our recommendations, and pleased with the spirit of co-operation the company has shown.

A case of deception

It is one thing to do a poor job of informing individuals of the purposes for which their information would be used, as three of the above-mentioned organizations did. It is quite another to deliberately misinform, as we found to be the case in a complaint against a market research firm.

This firm mails questionnaires for what it calls "consumer product surveys" to households across Canada. The questionnaires ask about household preferences among various categories of products. The literature accompanying each questionnaire explains the purpose of the survey strictly in terms of "fact-finding," seeking householders' "opinion" and understanding consumer "preferences and attitudes," all with a stated view to improving the quality, life and value of products.

However, the surveys were truly intended for the purpose of selling products to the survey respondents. What the survey firm mainly intends to do with the personal information it collects in the questionnaires is compile customized mailing lists, which it will then give to the third-party companies that have commissioned the given survey. These commissioning companies will then attempt to sell products to the survey respondents by directly marketing them according to the information they have provided in the questionnaires.

The *PIPED Act* says that an organization has to identify its true purposes for collecting personal information. It also says that consent to the collection of personal information must not be obtained through deception.

If an organization intends to give information it collects to direct marketers, it has to say so, in no uncertain terms and in a manner that people can reasonably understand. In the survey literature in question, there is neither an explicit statement nor even a reasonably understandable implication to the effect that personal information of individual respondents will be disclosed to third parties.

If an organization intends to give information it collects to direct marketers, it has to say so...

The questionnaire does ask for the respondent's consent to further mailings and offers, but says nothing about where such communications would come from. In the absence of any indication that the survey firm intends to share the respondent's mailing address with other possible mailers, the most reasonable inference would be that any further mailings would come from the same source as the original – that is, from the survey firm itself.

Furthermore, the consent mechanism is a problem in itself. Given that many of the survey questions are highly sensitive in nature (notably, several have to do with personal health and finances), the "opt-in" form of consent should be used in the circumstances. But the consent mechanism has two check-off boxes, one for "yes" and the other for "no", and is thus ambiguous as to the form of consent intended. What happens in fact, however, in the not-infrequent cases where the respondent checks off neither box, is that the individual is presumed to give consent to further mailings. Thus, the survey firm is using the "opt-out" form of consent in a situation that clearly calls for "opt-in."

The survey literature also does mention that companies have commissioned the survey. However, it does not name the commissioning companies. Nor does it in any discernible way suggest that these anonymous companies are direct marketers, or that what they have in effect commissioned from the survey firm is the collection of prospective customers' personal information on

their behalf. Indeed, there is nothing in the literature that gives the individual householder any substantial grounds to believe that the survey is anything other than what it purports up front to be – that is, strictly a fact-finding, opinion-seeking market study aimed at product improvement.

On the basis of such a description, respondents might reasonably expect that the survey's sponsors would receive results in the form of aggregated, anonymized analytical data. But respondents are given no legitimate reason to expect, and every good reason to resent, that as a result of their participation in the survey they may soon be subject to intrusive and unwanted direct-marketing efforts by third-parties who have been made privy to their sensitive personal information.

It may seem paradoxical to some that, despite the overwhelming case against the survey firm on these and other counts, what troubled us most was evidence of the firm's *compliance* with the *Act*.

The firm does, in fact, have an official written privacy policy pertaining to its household surveys posted on its Web site. This policy does a relatively good job of identifying the true purposes for collecting the survey information. However, not only is this policy not included or otherwise reflected in the survey literature mailed to households, but it is not made reasonably accessible to householders. The survey literature does not even mention the existence of the Web site, let alone that of the policy.

What troubled us specifically were the implications of the vast discrepancy in compliance between the Web site and the survey literature. In the letters of findings, the former Commissioner raised the concerns as follows:

> *"Why would [the firm] make reasonably clear in a remote and unadvertised privacy policy, but not at all clear in survey materials actually provided to individuals, that respondents' personal information would be disclosed to third parties for marketing purposes? Why in the survey materials would [the firm] explain the purposes of its surveys only in such limited terms as fact-finding, opinion-gathering, and product quality improvement, and relegate to a document that*

no one would ordinarily ever see the further purpose of direct marketing by third parties? Indeed, why would [the firm] take pains to formulate a more or less compliant privacy policy and then not draw attention to that policy when it truly mattered, in effect hiding the policy from customers?

"In brief, I find it difficult to comprehend this discrepancy, except in terms of deception. [The firm] has suggested that its survey materials serve to produce a reasonable expectation of disclosure to, and direct-marketing by, third parties. I cannot see, however, that any previously unsuspecting person could reasonably infer such a purpose from the scant, vague, and misleading indications provided. Rather, in my considered view, far from being conducive to a reasonable understanding of how personal information will be used or disclosed, the survey materials serve only to deceive individuals as to the true purposes of the surveys and to detract from the fairness of [the firm's] collection of personal information."

An advocacy group's expectations about consent

The *PIPED Act* states, at Principle 4.3.5 of Schedule 1, that the reasonable expectations of the individual are relevant in matters of consent. But it does not elaborate.

Rather, it leaves us the difficult task of interpreting this provision. In the circumstances of any consent-related complaint, it is often up to the Commissioner to determine the reasonableness of a complainant's expectations and the extent of their relevance. Fortunately, fairly early in the life of the *Act*, a body of complaints arose that we found useful in formulating a general position on what an individual may reasonably expect in matters of consent.

An individual filed complaints on behalf of an advocacy group against two banks, a telecommunications company, and a company that ran a frequent-buyer program. All the complaints were basically the same – that the organizations in question were not obtaining valid informed consent from individuals to disclosures of their personal information for marketing purposes.

The complaints consisted of two main allegations. The first was that the organizations were not making reasonable efforts to inform clients that their personal information was to be disclosed to third parties for secondary marketing purposes – that is, purposes additional to those for which the information needed to be collected in the first place. The complainant's contention was that, if individuals were not being properly informed of secondary purposes, the organizations had no valid basis for presuming the individual's consent to such purposes. The second main allegation was that, despite their reliance on the "opt-out" form of consent, the organizations were not providing reasonable opportunities for individuals to opt out of third-party marketing.

To us, these assumptions clearly represented "expectations" on the complainant's part.

As interesting as the allegations themselves were their underlying assumptions, which the advocacy group had presented in a position statement supporting the complaints. To us, these assumptions clearly represented "expectations" on the complainant's part. Before determining whether or not the organizations in question were in compliance with the relevant consent provisions of the *Act*, we thought it prudent to consider whether the group's expectations regarding consent were themselves reasonable in relation to the *Act*.

After analyzing them, the former Commissioner concluded that the group's expectations were entirely reasonable. Notably, the former Commissioner found it reasonable to expect the following from organizations that use or disclose personal information for secondary purposes:

- It is not enough to identify purposes in privacy policy documents and make such documents generally available. An organization should bring its secondary purposes directly to the attention of the individual at the time of

collecting personal information. During an application or a subscription process, for example, the individual should be presented with the necessary information and should not be referred to sources not immediately at hand. (These expectations are supported by Principles 4.2.3 and 4.3.1 of the *Act*, which instruct that identification of purposes and seeking of consent be direct and coincident with the collection of personal information.)

- Purposes should be stated in clear, plain language understandable to the ordinary consumer and in adequate detail for the consumer to appreciate the nature and extent of the intended collections, uses, and disclosures. (These expectations are supported by Principle 4.3.2, which instructs that purposes be stated in such a manner that the individual can reasonably understand how personal information will be used or disclosed.)
- If purposes are identified in writing, the individual should not be required to read fine print in dense passages.

Where an organization intends to presume the individual's consent to secondary purposes, the organization should provide a convenient opportunity for the individual to opt out. The opportunity and the procedure for opting-out should likewise be brought to the individual's attention at the time of collecting the personal information. The opting-out procedure should be easy, immediate, and inexpensive.

On this basis, and upon investigation of the actual policies and practices of the organizations, the Commissioner concluded that two of the complaints were well-founded and two were not. The former Commissioner found that the telecommunications company was not making any disclosures of the kind alleged, since it was prohibited from doing so by the CRTC. One bank was indeed disclosing personal information for secondary marketing purposes as alleged, but the former Commissioner found it to be making reasonable efforts on the whole to inform account applicants of the practice, obtain their consent to it, and provide them with an opt-out opportunity.

In the well-founded cases, the non-compliance of the frequent-buyer program was largely a matter of inconsistency in enrolment procedures. The case of the second bank, however, was much more serious. This bank's efforts at obtaining informed consent from account applicants did not in any respect meet the requirements of the *Act* or the reasonable expectations of the individual. In the letter of findings, the former Commissioner commented on the various materials used by the bank to communicate purposes, and on the nature and extent of the failed compliance in this case:

> *"The wording ... is so broad in each case as to virtually preclude understanding, unless the individual is to understand that the bank intends to use personal information however it may see fit and disclose it to whomever it may see fit. This would hardly be a purpose that any reasonable person would expect or consider appropriate in any circumstances."*

By positive contrast, it should be noted that, in the case of the first bank, the former Commissioner complimented the bank on its approach to obtaining informed consent from account applicants. For those applying in person at branches, this bank's application procedure involved sitting the individuals down, providing them with the appropriate privacy information on the spot, drawing their attention specifically to statements of secondary marketing purposes, asking whether they consented or not to specific marketing practices, and recording and abiding by their responses. We regard such procedure as exemplary, amounting to the positive form of consent that we prefer.

Consent to secondary purposes

What follows is a summary of the deliberations to date in cases relating to consent to secondary purposes.

- Positive or opt-in consent is always to be preferred as the form of consent that is strongest, most respectful of individuals, and best in keeping with the spirit of the *Act*. Organizations are encouraged to adopt this form of consent exclusively.

- Positive or opt-in consent to secondary purposes is a requirement in situations where the personal information is sensitive in itself or where there is a significant potential for the information to be rendered sensitive in the context of the information-handling activities.
- Since the *Act* indicates that personal information of a financial or medical nature is almost always to be considered sensitive, these types of information will almost always be deemed to warrant positive consent. However, since the *Act* also stipulates that any personal information may be sensitive in a given context, no further attempt should be made to precisely define the notion of sensitivity. Rather, the context should be considered in each case, with a view to determining the potential for sensitivity.
- Two prime considerations in determining the potential for sensitivity of personal information are the intent to disclose the information to third parties and the intent to categorize or otherwise process the information according to personal criteria.
- Negative or opt-out consent, also known as presumed consent, despite being the weaker and less preferable form, is recognized under the *Act* as being acceptable in certain circumstances. The scope of circumstances in which this form of consent is allowable will remain limited.
- An organization's use of the negative or opt-out form of consent to secondary purposes will be deemed justified only under the following conditions:
    - The personal information must be of a demonstrably non-sensitive nature and context and must be identified by item or type.
    - If the information is to be disclosed to third parties, the parties must be identified by name or type.
    - The organization must state its purposes in full accordance with Principles 4.2, 4.2.3, 4.3.1, and 4.3.2 and with the individual's reasonable expectations as deemed relevant in Principle 4.3.5. Specifically, the identified purposes must be brought directly to the individual's attention, either orally or in writing, at the time the personal information is collected (e.g., during the subscription, application, or enrolment process); in clear, specific, unambiguous terms; in a format easy to read (where text is used); and in a manner conducive to the

individual's understanding of how exactly the personal information is to be used or disclosed.

- The organization must provide an appropriate "opt-out" mechanism – that is, a convenient opportunity and procedure for withdrawal of consent. The mechanism must be brought to the individual's attention at the time the personal information is collected and should be inexpensive, easy to execute, and immediately effective in withdrawing consent. Where feasible, it should include a toll-free number.

INCIDENTS UNDER THE *PIPED ACT*

Checking up on telephone calls

A journalist contacted the Office about a survey being conducted on behalf of a telephone company by a research firm. It appeared as though the company was gathering information from customers about their telephone calls.

The research firm had a contract with the telephone company to carry out random checks for quality assurance purposes. The telephone company provided the firm with the phone number of customers who had made calls seeking assistance by dialing "0" or "411." The firm was not given the names of the customers or other identifying information. The company has a non-disclosure contract with the research firm, which requires the firm to destroy the information it collects once the results of the survey are compiled.

The former Commissioner was satisfied when it was determined that the telephone company was complying with a CRTC requirement to conduct regular quality of service measurements of the accuracy of Directory Assistance services.

Dumpster find

A bank alerted the Office that confidential client documents had been found in a dumpster located near a branch that had closed some time earlier. The building had been leased to a new tenant and was being renovated. Apparently the renovators found the documents during the reconstruction and disposed of them. Upon hearing of the matter, the media retrieved some of the documents from the dumpster.

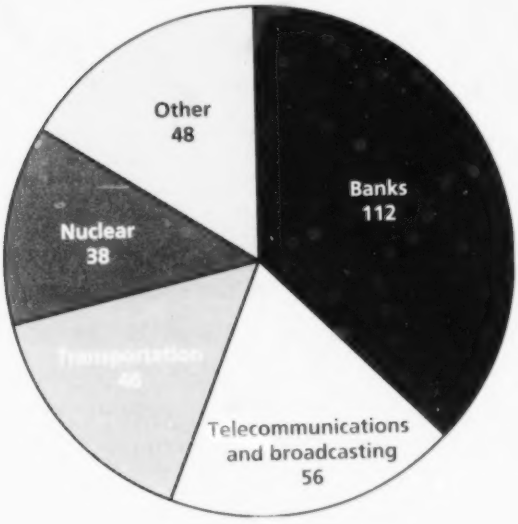
The bank took prompt action as soon as it became aware of the situation by recovering all of the documents from the dumpster and the journalists; then it verified that no other bank documents remained in the building. The bank also informed each of the affected customers, either in person or in writing, of the incident and of the steps it had taken to recover the documents. In addition, the bank apologized to each customer and assured each one that all of their information had been recovered.

It was determined that the branch in question was amalgamated with another, and a private company on contract to the bank was tasked with sorting through and processing records. The bank has established procedures for this, but the private company did not follow these properly, with the result that some documentation was not appropriately classified and was disposed of incorrectly. The bank subsequently clarified procedures with the private company.

The former Commissioner was satisfied that the bank acted promptly and appropriately in dealing with this sensitive situation.

Complaints Received by Sector

January 1, 2002 to December 31, 2002



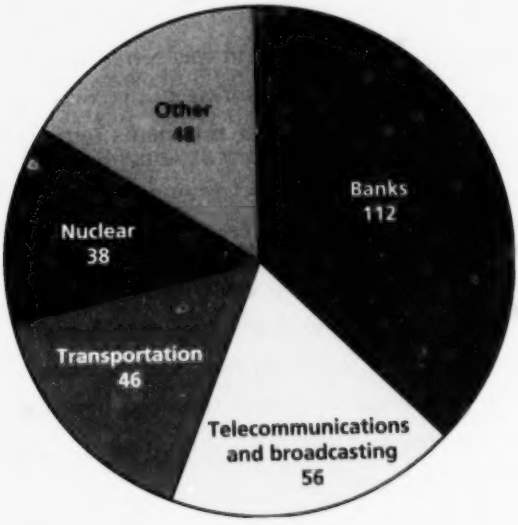
Inquiries under the *PIPED Act*

January 1, 2002 to December 31, 2002: 8,381

We will attempt to provide a breakdown of these inquiries by subject in future Annual Reports.

Complaints Received by Sector

January 1, 2002 to December 31, 2002



Inquiries under the *PIPED Act*

January 1, 2002 to December 31, 2002: 8,381

We will attempt to provide a breakdown of these inquiries by subject in future Annual Reports.

PRIVACY PRACTICES AND REVIEWS

The *Personal Information Protection and Electronic Documents (PIPED) Act* enables the Commissioner to audit the compliance of private sector organizations if there are reasonable grounds to believe that they are in contravention of the *Act* or are not following a recommendation set out in Schedule 1 (ten principles). The Privacy Practices and Reviews (PP&R) Branch will conduct such compliance reviews and audits under section 18 of the *PIPED Act*, following accepted standard audit objectives and criteria. During the period under review, there were a number of issues that were brought to the Commission's attention that were successfully resolved without the necessity of conducting an audit. For example, Office of the Privacy Commissioner staff met and advised representatives of an industry association on the viability of obtaining direct consent and the proposed contents of such a consent form. We provided guidance to a business with respect to the use of the SIN as an identifier and the use of opt-out consent. As well, we provided a comprehensive review and analysis of a corporate privacy policy.

Apart from those issues, the former Commissioner was not aware of any other concerns that would provide sufficient grounds to initiate an audit under the law.

Nevertheless, the PP&R Branch has been involved in consulting with and providing advice to private sector organizations that come under the jurisdiction of the *PIPED Act*. It has also assisted those organizations that are not currently governed by the *Act* but that are preparing for January 1, 2004, when the *Act* will begin to apply to them.

IN THE COURTS

Under section 14 of the *Personal Information Protection and Electronic Documents (PIPED) Act*, an individual complainant has a right, following the Commissioner's investigation, to apply to the Federal Court of Canada for a hearing in respect of any matter that is referred to in the Commissioner's report. These matters must be among those in the listed Schedule clauses and sections of the *PIPED Act*.

Section 15 of the *Act* allows the Commissioner to apply to appear in Federal Court. The Commissioner may, with the consent of the complainant, apply directly to the court for a hearing in respect of any matter covered by section 14; appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or, with the leave of the Court, appear as a party to any section 14 hearing.

Following is a list of all *PIPED Act* applications in the courts from January 1, 2001 to December 31, 2002:

Mathew Englander v. Telus Communications Inc.

Federal Court File No. T-1717-01

This is the first application for judicial review to be filed in the Federal Court under the *PIPED Act*. Mr. Englander argues that Telus uses and discloses customers' names, addresses and telephone numbers in its white pages directories and otherwise, without customers' knowledge and consent, and inappropriately charges customers for choosing to have their telephone number "non-published." He claims that these actions by Telus contravene subsections 5(1) and (3) of the *PIPED Act*, as well as several clauses of Schedule 1 of the *PIPED Act*.

Status

This Application was dismissed on June 2, 2003.

Ronald G. Maheu v. the Attorney General of Canada and IMS Health Canada

Federal Court File No. T-1967-01

Ronald Maheu applied for a hearing in the Federal Court arguing that IMS Health Canada improperly discloses personal information by selling data on physicians' prescribing patterns without their consent.

Status

Mr. Maheu filed an Amended Notice of Application in March 2002. IMS brought a motion seeking either to strike out the Application on the grounds that it was brought for an improper purpose or to have Mr. Maheu post security for costs. The Court ordered Mr. Maheu to post security for costs in the amount of $12,000 and noted that there appeared to be reason to believe that Maheu was using the *Act* for a collateral and improper purpose given that his own personal information was not at issue. On appeal, the former Commissioner appeared to assist the Court with respect to the proper interpretation of the *PIPED Act*, explaining that an individual may file a complaint concerning an organization's information practices regardless of whether that organization collects, uses or discloses personal information about the individual complainant. The Federal Court agreed with this position and granted Mr. Maheu's appeal on January 3, 2003. This decision is currently being appealed, and the original Application continues to proceed in Trial Division.

Diane L'Ecuyer v. Aéroports de Montréal

Federal Court File No. T-2228-01

Diane L'Ecuyer complained that Aéroports de Montréal had sent copies of a letter of response to access requests she had made to two union representatives and an employee relations co-ordinator and had, therefore, disclosed personal information without her consent. The former Commissioner investigated her complaint and, among the findings, recommended that individuals must be allowed to judge for themselves whether or not to share such a response with others.

Status

Madame L'Ecuyer applied to Federal Court on December 18, 2001, seeking an Order that the organization correct its practices to conform with the *PIPED Act* and that the organization publish a notice stating any action taken or proposed to be taken to correct its practices. On May 13, 2003 the Trial Division released its decision, finding that the issue arose from the administration of a collective agreement and therefore was not within the jurisdiction of the Privacy Commissioner. Madame L'Ecuyer filed an appeal of that decision on June 5, 2003 and the Privacy Commissioner is preparing to apply for leave to intervene in that appeal.

Nancy Carter v. Inter.net Canada Limited

Federal Court File No. T-1745-02

Nancy Carter contacted the Office with concerns about the practice(s) of her Internet Service Provider (ISP). During a billing dispute with the complainant, the ISP had suspended her access to e-mail, but continued to keep the account active and accepted new e-mails into the mailbox. The claimant argues that she was therefore denied access to her personal information contrary to the *PIPED Act*, and lost a valuable business opportunity as a result. She is seeking damages under the *PIPED Act*.

Status

A settlement was reached in this case and accordingly a Notice of Discontinuance was filed on June 5, 2003.

Sylvain Gagné v. Bell Canada

Federal Court File No. T-1971-02

Sylvain Gagné complained to the Office that (a) that he had been denied access to some of his personal information and (b) of the improper disclosure of the personal information of others. Although the former Commissioner found the denial of access complaint to be not well-founded, agreeing that exemptions under 7(1)(b) and 9(3)(c.1) had been correctly applied, the complaint about the disclosure of personal information was well-founded and the former Commissioner issued recommendations as to change of practices.

Status

The Notice of Application was filed in Federal Court on November 25, 2002, requesting a variety of relief, including access to the withheld documents, damages to those affected, and Orders enforcing the Office's recommendations.

Bell Canada has now agreed to follow the Office's recommendations, and thus a Notice of Discontinuance was filed on March 14, 2003.

Dale Stuart v. the Toronto Dominion Bank

Federal Court File No. T-290-02

Dale Stuart believed that information about his banking affairs had been disclosed by employees of the TD Bank to his employer without Mr. Stuart's knowledge or consent.

Status

This application was discontinued by Mr. Stuart on December 2, 2002.

Yukon Hospital Corporation v. Attorney General of Canada

Federal Court File No. T-1814-02

This action was initiated in response to the former Commissioner's determination that he had jurisdiction under section 4(1)(b) to conduct an investigation of a complaint filed against the Yukon Hospital Corporation.

Status

A complaint was filed with this Office under the *Privacy Act*. Although the Yukon Hospital Corporation is governed by the *PIPED Act*, the complaint was originally made under the *Privacy Act*. After discussions with the Applicant to this effect, the former Commissioner withdrew his decision to investigate the complaint. Court proceedings were discontinued on February 21, 2003.

Keith Vanderbeke v. Royal Bank of Canada

Federal Court File No. T-2185-02

Keith Vanderbeke contacted the Office complaining that the Royal Bank of Canada had denied him access to three documents pertaining to a commercial mortgage for which he personally was the guarantor.

Status

In the application, the claimant is specifically seeking (among other things) interpretive Orders relating to the *PIPED Act*: an Order that a private corporation may be an "identifiable individual" under the *PIPED Act* with attendant access rights; and an Order that private corporation banking documents should be considered personal documents where a natural person has provided a personal guarantee to the creditor. It is uncertain whether this aspect will be allowed to continue because, among other things, the part of the Application apparently brought pursuant to section 14 of the *PIPED Act* improperly seeks review of the former Commissioner's findings. Under section 14 of the *PIPED Act*, the only proper respondent is the Royal Bank of Canada.

Part Three

Corporate Services

On April 1, 2002, the Office of the Privacy Commissioner of Canada ceased to share corporate services with the Office of the Information Commissioner of Canada, and established its own Corporate Services Branch.

The Corporate Services Branch provides advice and services in the areas of finance, human resources, information technology and administration to the Office's senior managers and staff.

As noted in the Foreword, the House of Commons Committee on Government Operations and Estimates has, in the course of examining the operations of the Office, uncovered a number of serious problems related to some of these areas. As well, the Office is the subject of reviews by both the Office of the Auditor General of Canada and the Public Service Commission of Canada.

I intend to use the results of these reviews to ensure that the Office is managed in a manner that is accountable to Parliament and respects the polices and regulations applicable to the public service.

At the beginning of fiscal year 2002-2003, the Office's budget was $11.1 million, the same as our budget for the previous year. During the course of the year,

our budget was adjusted upward by $773,000, primarily to offset increased legal costs, costs associated with the Government's new Privacy Impact Assessment Policy and collective bargaining salary increases, for a total budget of $11.9 million.

Our expenditures totalled $12.2 million. We exceeded our budget by $240,000 largely due to changes in accounting practices in order to be consistent with the principles of accrual accounting in the federal government.

The Office is currently reviewing its financial resources, in conjunction with the Treasury Board Secretariat, to ensure that it has the resources needed to fulfill its obligations in fiscal year 2003-2004 and beyond in anticipation of the full and final implementation of the *PIPED Act* on January 1, 2004.

Resources

April 1, 2002 to March 31, 2003

	Expenditure Totals ($)	% of Totals
Privacy Act	5,208,588	43%
PIPED Act	5,582,722	46%
Corporate Services	1,367,778	11%
Total	**12,159,088**	**100%**

Note that as of March 2003 there were 103 full-time staff at the Office of the Privacy Commissioner of Canada.

Detailed Expenditures[1]

April 1, 2002 to March 31, 2003

	Privacy Act	*PIPED Act*	Corporate Services[2]	Total
Salaries	3,462,955	2,845,391	808,513	**7,116,859**
Employee Benefits Program	657,386	595,000	240,220	**1,492,606**
Transportation and Communication	284,228	352,412	67,005	**703,645**
Information	25,649	315,406	34,592	**375,647**
Professional Services	679,897	700,870	65,526	**1,446,293**
Rentals	12,840	2,202	11,648	**26,690**
Repairs and Maintenance	8,607	41,249	5,447	**55,303**
Materials and Supplies	44,328	5,012	51,699	**101,039**
Acquisition of Machinery and Equipment	29,100	725,180	83,128	**837,408**
Other Subsidies and Payments	3,598	-	-	**3,598**
Total	**$5,208,588**	**$5,582,722**	**$1,367,778**	**$12,159,088**

Notes:

[1] Total expenditure figures are consistent with public accounts.

[2] Effective April 1, 2002, Corporate Services is part of this Office and resources are no longer shared with the Office of the Information Commissioner of Canada.

our budget was adjusted upward by $773,000, primarily to offset increased legal costs, costs associated with the Government's new Privacy Impact Assessment Policy and collective bargaining salary increases, for a total budget of $11.9 million.

Our expenditures totalled $12.2 million. We exceeded our budget by $240,000 largely due to changes in accounting practices in order to be consistent with the principles of accrual accounting in the federal government.

The Office is currently reviewing its financial resources, in conjunction with the Treasury Board Secretariat, to ensure that it has the resources needed to fulfill its obligations in fiscal year 2003-2004 and beyond in anticipation of the full and final implementation of the *PIPED Act* on January 1, 2004.

Resources

April 1, 2002 to March 31, 2003

	Expenditure Totals ($)	% of Totals
Privacy Act	5,208,588	43%
PIPED Act	5,582,722	46%
Corporate Services	1,367,778	11%
Total	**12,159,088**	**100%**

Note that as of March 2003 there were 103 full-time staff at the Office of the Privacy Commissioner of Canada.

Detailed Expenditures[1]

April 1, 2002 to March 31, 2003

	Privacy Act	*PIPED Act*	Corporate Services[2]	Total
Salaries	3,462,955	2,845,391	808,513	**7,116,859**
Employee Benefits Program	657,386	595,000	240,220	**1,492,606**
Transportation and Communication	284,228	352,412	67,005	**703,645**
Information	25,649	315,406	34,592	**375,647**
Professional Services	679,897	700,870	65,526	**1,446,293**
Rentals	12,840	2,202	11,648	**26,690**
Repairs and Maintenance	8,607	41,249	5,447	**55,303**
Materials and Supplies	44,328	5,012	51,699	**101,039**
Acquisition of Machinery and Equipment	29,100	725,180	83,128	**837,408**
Other Subsidies and Payments	3,598	-	-	**3,598**
Total	**$5,208,588**	**$5,582,722**	**$1,367,778**	**$12,159,088**

Notes:

1 Total expenditure figures are consistent with public accounts.

2 Effective April 1, 2002, Corporate Services is part of this Office and resources are no longer shared with the Office of the Information Commissioner of Canada.

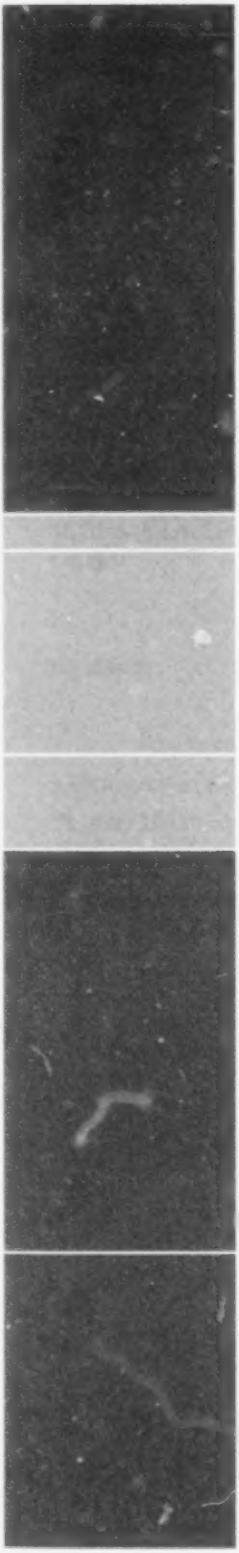
Commissaire à la protection
de la vie privée du Canada

Privacy Commissioner
of Canada

Vie privée

RAPPORT ANNUEL

AU PARLEMENT 2002-2003



Commissaire à la protection
de la vie privée du Canada

Privacy Commissioner
of Canada

Vie privée

RAPPORT ANNUEL

AU PARLEMENT 2002-2003

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-8210, 1-800-282-1376
Téléc. (613) 947-6850
ATS (613) 992-9190

© Ministre des Travaux publics et Services gouvernementaux Canada 2003
N° de cat. IP30-1/2003
ISBN 0-662-67544-4

Cette publication est également disponible sur
notre site Web à **www.privcom.gc.ca**

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Téléc. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Septembre 2003

L'honorable Daniel Hays, sénateur
Président
Sénat du Canada
Ottawa

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour les périodes du 1er avril 2002 au 31 mars 2003 conformément à la *Loi sur la protection des renseignements personnels* et du 1er janvier au 31 décembre 2002 conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Veuillez agréer, Monsieur, l'expression de mes sentiments distingués.

Commissaire à la protection
de la vie privée du Canada
par intérim,

Robert Marleau

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Téléc. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Septembre 2003

L'honorable Peter Milliken, député
Président
Chambre des communes
Ottawa

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour les périodes du 1er avril 2002 au 31 mars 2003 conformément à la *Loi sur la protection des renseignements personnels* et du 1er janvier au 31 décembre 2002 conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Veuillez agréer, Monsieur, l'expression de mes sentiments distingués.

Commissaire à la protection
de la vie privée du Canada
par intérim,

Robert Marleau

Table des matières

Préface 1

Aperçu 3

Lois provinciales essentiellement similaires 15

Partie I - Rapport concernant la *Loi sur la protection des renseignements personnels* 19

Introduction 19
Enquêtes et demandes de renseignements 20
Plaintes en vertu de la *Loi sur la protection des renseignements personnels* 21
Définition de conclusions aux termes de la *Loi sur la protection des renseignements personnels* 23
Sommaires de cas choisis en vertu de la *Loi sur la protection des renseignements personnels* 24
Incidents visés par la *Loi sur la protection des renseignements personnels* 39
Communications dans l'intérêt public 41
Examens et pratiques en matière de vie privée 50
Évaluation des facteurs relatifs à la vie privée 52
Devant les tribunaux 57

Partie II - Rapport concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* 63

Introduction 63
Enquêtes et demandes de renseignements 64
Définition de conclusions en vertu de la *LPRPDÉ* 65
Sommaires de cas choisis en vertu de la *LPRPDÉ* 66
Incidents visés par la *LPRPDÉ* 101
Examens et pratiques en matière de vie privée 104
Devant les tribunaux 105

Partie III - Services de gestion 111

Préface

D'aucuns trouveront peut-être singulier que ce soit moi qui présente le rapport annuel de l'exercice 2002-2003. En effet, j'ai été nommé commissaire à la protection de la vie privée par intérim en juillet de cette année bien après la fin de la période visée par ce rapport. Je ne peux, par conséquent, m'attribuer le mérite des travaux rapportés ici. Cependant, à y regarder de près, cette situation ne pose pas vraiment problème. Le Commissariat à la protection de la vie privée ne se limite pas au commissaire, et d'ailleurs, même si j'avais occupé mes fonctions actuelles tout au long de l'exercice 2002-2003, il serait illusoire de dire que ce rapport est « mon » rapport annuel. Il reflète plutôt le travail de personnes très talentueuses et dévouées.

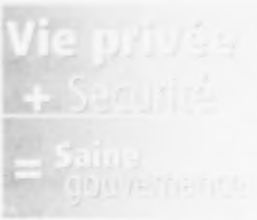
Le Commissariat traverse une période particulièrement mouvementée de son histoire. *A priori*, la tâche de la protection de vie privée est plus ardue que jamais, en raison de la nouvelle loi pour le secteur privé, d'un vaste éventail de mesures proposées en matière de sécurité et de lutte contre le terrorisme, et de la propagation de technologies sans cesse améliorées qui portent atteinte à la vie privée.

Pour compliquer les choses, le Commissariat a traversé une période durant laquelle il a fait l'objet d'un examen public minutieux et connu des perturbations organisationnelles. Le Comité permanent des opérations gouvernementales et des prévisions budgétaires de la Chambre des communes a mené une enquête relativement à diverses questions opérationnelles et administratives qui se sont posées au Commissariat et il a relevé un certain nombre de problèmes sérieux. Bien que ce processus de supervision parlementaire soit important et nécessaire, on ne saurait nier le fait qu'il a rendu difficile la tâche du personnel du Commissariat de mener à bien son travail, surtout si l'on considère l'attention médiatique qui l'a accompagné.

J'ai accepté le poste de commissaire à la protection de la vie privée à titre intérimaire, afin de conduire le Commissariat dans son processus de reconstruction et de restauration des liens qu'il entretient avec le Parlement et la population canadienne. Nous avons maintenant pour tâche de regagner la confiance du Parlement et des intervenants en matière de vie privée, de prouver aux Canadiens et aux Canadiennes que nous sommes en mesure de leur fournir des services de haute qualité en ce qui a trait à la protection de leurs droits à la vie privée, de veiller à ce que les organisations comprennent leurs obligations et les citoyens leurs droits, lorsque la *Loi sur la protection des renseignements personnels et les documents électroniques* entrera pleinement en vigueur le 1er janvier 2004.

J'ai été impressionné par l'engagement des employés du Commissariat et je suis heureux de collaborer avec eux en cette période stimulante de l'histoire de l'organisme. Je demeure confiant qu'un regain d'enthousiasme pour la défense du droit à la vie privée et un centre d'excellence pour sa protection et sa promotion naîtront de cette période de renouveau.

Aperçu



Il est habituel de faire la présentation d'un rapport annuel en formulant quelques observations afin de susciter la réflexion. Dans le cas du présent rapport, il ne s'agit pas d'une présentation futile. La période couverte s'est avérée particulièrement importante pour le droit à la vie privée.

D'une part, le droit à la vie privée dans notre société a été quelque peu menacé. Ce qui n'est certes pas nouveau ; le droit à la vie privée n'a jamais été quelque chose que nous pouvons prendre pour acquis, et cela est d'autant plus vrai depuis l'avènement de l'informatisation, qui nous force à tout mettre en œuvre pour le préserver. Mais si la menace qui plane sur le droit à la vie privée n'est pas nouvelle, elle s'est bel et bien accentuée Les forces qui rongent le droit à la vie privée depuis dix ans — les avancées technologiques liées à la collecte, au traitement, au couplage et à l'analyse des renseignements personnels, la pression grandissante exercée pour que l'on identifie et authentifie les parties à des transactions électroniques et la campagne de prévention du crime et du terrorisme — ont été particulièrement puissantes au cours de la dernière année.

Les mesures de sécurité publique pour lutter contre le crime et le terrorisme ont sans aucun doute constitué le défi le plus grave et le plus évident. Elles

posent également un défi des plus indéniables pour les défenseurs du droit à la vie privée et les commissaires à la protection de la vie privée qui, ce faisant, doivent tenir une position délicate entre la protection du droit à la vie privée et le risque de faciliter la vie des criminels et des terroristes.

Mais, en fait, les autres forces qui menacent la vie privée ne posent pas moins de défi et le fait d'avoir à y faire face et d'œuvrer en faveur du droit à la vie privée nous met souvent dans des situations tout aussi délicates. Le couplage des données permet d'appréhender les personnes qui tentent de frauder le système. Les cartes d'identité peuvent rendre la tâche plus difficile à une personne qui cherche à utiliser frauduleusement votre carte de crédit. Les dossiers de santé électroniques peuvent faciliter le diagnostic et le traitement des maladies et prévenir des erreurs médicales pouvant entraîner des coûts importants ou causer la mort. Le fait de donner aux chercheurs accès aux renseignements personnels sur la santé peut donner lieu à des recherches en vue de prolonger la vie et réduire la souffrance.

Personne ne contesterait les objectifs de ces mesures. Mais le droit à la vie privée n'est pas simplement un luxe ou une extravagance égoïste que l'on peut jeter dès que quelqu'un prétend qu'elle est une entrave à quelque autre objectif social important, qu'il s'agisse de la sécurité ou de la santé publique ou même de la vie personnelle ou de la mort. Le droit à la vie privée est la pierre angulaire de la liberté individuelle. Elle forme un équilibre dynamique avec les autres besoins sociaux que nous avons. Pour préserver le droit à la vie privée, il importe d'analyser minutieusement toute mesure censée nous procurer quelque autre avantage social, de manière à s'assurer que l'équilibre est maintenu.

Au cours de la dernière année, nos efforts ont donné des résultats divers. Nous avons continué de gérer un volume important de plaintes et de veiller à ce que les Canadiens et les Canadiennes jouissent d'une pleine protection de leurs droits en vertu de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et les documents électroniques*. À l'égard de questions d'ordre plus général liées à la promotion et à la protection du droit à la vie privée, nous avons réalisé quelques progrès

significatifs. Nous avons aussi connu certains reculs et, dans quelques domaines, nous avons été forcés de repenser notre approche.

À l'égard de questions d'ordre plus général liées à la promotion et à la protection du droit à la vie privée, nous avons réalisé quelques progrès significatifs.

L'intervention du Commissariat concernant le projet de base de données sur les passagers des compagnies aériennes de l'Agence des douanes et du revenu du Canada a été couronnée de succès.

Cette base de données, telle que proposée au départ, devait contenir des renseignements très détaillés sur les voyages à l'étranger effectués par les Canadiens et les Canadiennes — où et avec qui ils voyagent, comment ils ont payé leurs billets, leurs adresses et numéros de téléphone et même leurs besoins particuliers en matière d'alimentation et de santé. On aurait conservé pendant sept ans cette information, qui aurait servi à un vaste éventail d'objectifs administratifs et d'objectifs liés à l'application de la loi.

Les répercussions de ce projet auraient été considérables et sans précédent. Des voyageurs respectueux de la loi auraient vu leurs activités habituelles, qui auparavant seraient passées inaperçues à moins qu'il n'y ait eu des motifs valables de s'en méfier, consignées et conservées dans un fichier à leur nom. Il en résulterait une autre perte de l'anonymat et du droit à la vie privée, un autre moyen pour l'État d'identifier, d'étiqueter et de surveiller des personnes innocentes, bref une autre atteinte au droit à la vie privée.

Après avoir analysé ce projet, notre personnel a conclu que les avantages supposés qu'il allait offrir sur le plan de la sécurité ne justifiaient pas la violation du droit à la vie privée qui allait en découler. Notre opposition, qui a reçu l'appui du public, a finalement incité la ministre du Revenu national à revoir le projet et, ce faisant, à en réduire considérablement l'incidence sur le droit à la vie privée.

Mais il faut plus qu'une réussite pour qu'une année soit exceptionnelle. Nous avons toujours des préoccupations concernant d'autres initiatives liées à la sécurité. Pensons notamment aux dispositions du projet de loi sur la sécurité publique permettant aux policiers de contrôler tous les passagers des transporteurs aériens au regard des mandats d'arrestation non exécutés ; aux propositions relatives à « l'accès légal » visant à accroître les pouvoirs de l'État en matière de surveillance des communications électroniques ; à la proposition concernant la carte d'identité nationale et au recours croissant par les forces policières à la surveillance vidéo des voies publiques.

Un conflit de longue date, entourant la confidentialité des données de recensement, semble en voie d'être résolue d'une manière qui va tout à fait à l'encontre des recommandations du Commissariat.

Depuis au moins 1905, on répète aux Canadiens et aux Canadiennes que les renseignements fournis dans le cadre des recensements demeurent confidentiels et servent uniquement à des fins statistiques. En fait, la *Loi sur la protection des renseignements personnels* permet aux Archives nationales de communiquer des renseignements personnels recueillis dans le cadre d'un recensement, 92 ans après que ce dernier a été réalisé. Cette disposition est demeurée en grande partie purement théorique jusqu'à tout récemment, dans la mesure où les seules données de recensement dont disposaient les Archives provenaient des quelques recensements effectués jusqu'en 1901. Les fonctionnaires du recensement ont affirmé que, depuis le recensement de 1906, les lois et les règlements les obligeaient à conserver les données confidentielles plutôt que de les transférer aux Archives.

Les historiens et d'autres chercheurs ont longtemps sollicité l'accès à ces documents. Or, cette année, le gouvernement, suivant les recommandations formulées par un groupe d'experts mais passant outre nos objections, a rendu publiques les données du recensement de 1906 et adopté une loi permettant la communication des données des autres années.

Le Commissariat avait favorisé un compromis qui aurait limité l'accès aux données aux chercheurs qui mènent une étude historique examinée par des

pairs et aux personnes qui désirent effectuer des recherches généalogiques sur leur propre famille. Le gouvernement a rejeté l'idée.

Ce qui nous préoccupe, c'est la promesse répétée de confidentialité. On a demandé aux Canadiens et aux Canadiennes de révéler des renseignements personnels aux recenseurs en leur laissant croire que tout demeurerait confidentiel. Le non respect de cette promesse pourrait diminuer la confiance que les Canadiens et les Canadiennes ont envers le gouvernement. Nous continuons d'espérer que la Chambre des communes tiendra compte de ce fait lorsqu'elle reprendra ce projet de loi, que le Sénat a adopté en mai.

En ce qui a trait à la surveillance vidéo des voies publiques, un autre enjeu important en matière de vie privée, nous avons conclu qu'il était essentiel d'adopter une nouvelle approche. L'ancien commissaire avait intenté un procès devant la Cour suprême de la Colombie-Britannique, alléguant que la surveillance vidéo, par la GRC, d'une rue publique de Kelowna contrevenait aux dispositions de la *Charte canadienne des droits et libertés*. Toutefois, le juge ne s'est pas du tout intéressé au fond de l'affaire. Statuant que le commissaire à la protection de la vie privée n'était simplement pas habilité à entamer une telle poursuite, il a rejeté l'affaire.

Nous nous trouvions donc dans une situation délicate. D'une part, la surveillance vidéo de lieux publics a de graves répercussions sur le droit à la vie privée, de sorte que l'idée de laisser simplement tomber l'affaire en raison d'un problème procédural ne nous semblait guère satisfaisante. D'autre part, peu importe ce que nous voulions, l'enjeu était devenu celui que la Cour avait adopté. Si nous avions appelé de la décision, l'appel n'aurait porté que sur ce point. Il nous aurait fallu des années pour traverser deux autres niveaux d'appel et ces procédures auraient nécessité beaucoup d'énergie de la part du Commissariat, ainsi qu'une quantité considérable de fonds publics, et ce sans que nous puissions obtenir des tribunaux une réponse sur l'enjeu essentiel de la surveillance vidéo. Certes, il est impératif de s'attaquer à la question, mais nous devons nous y prendre autrement. Par conséquent, nous avons abandonné l'action en justice, mais nous poursuivrons cette affaire avec détermination.

Au cours de la dernière année, nous avons été frappés par le fait que bon nombre de nos préoccupations en matière de vie privée étaient liées à l'anonymat et à son pôle contraire, l'identité. La capacité de mener la plupart de nos activités quotidiennes dans l'anonymat est un des moyens dont nous disposons pour exercer un contrôle sur les renseignements qui nous concernent. Une personne peut bien avoir une vie privée même si elle passe le plus clair de son temps en public, pourvu que ses activités ne puissent pas être reliées entre elles et qu'aucun lien ne puisse pas être établi entre cette personne et ses activités. La capacité de relier des activités entre elles et de les relier à une personne identifiable constitue l'essentiel de l'établissement de profils et de la surveillance.

Au cours de la dernière année, nous avons été frappés par le fait que bon nombre de nos préoccupations en matière de vie privée étaient reliées à l'anonymat et à son pôle contraire, l'identité.

Cette perspective regroupe les préoccupations que nous avons à l'égard de questions différentes en apparence, telles que l'authentification des clients effectuant des transactions électroniques, les systèmes biométriques de reconnaissance des visages dans les aéroports, les bases de données sur les voyageurs et la carte d'identité nationale.

C'est là l'idée que nous avons tenté de faire valoir devant le Comité permanent de la citoyenneté et de l'immigration de la Chambre des communes lors des audiences portant sur la question de savoir si le Canada a besoin d'instituer une carte d'identité nationale. Nous avons fondé notre argument sur le fait qu'une telle carte (quels que soient les détails de la proposition, et aucune proposition réelle n'a encore été présentée) aurait peu d'incidence sur le règlement des vrais problèmes, qu'elle présenterait un défi

de taille sur les plans financier et pratique quant à sa mise en œuvre et aurait de graves répercussions sur le droit à la vie privée.

Si le Commissariat défend un large éventail d'intérêts et s'efforce d'éclairer le Parlement sur toutes les questions liées au droit à la vie privée, il n'en demeure pas moins que le cœur et l'âme de son travail résident dans le système des droits exécutoires relatifs à la vie privée prévus aux termes de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

À cet égard, l'année 2003 est des plus remarquables. Tout d'abord, elle marque le 20e anniversaire de la *Loi sur la protection des renseignements personnels*. Ce qui nous porte à réfléchir non seulement sur la dernière année, mais aussi sur les vingt dernières années et tout particulièrement sur le modèle de protection du droit à la vie privée sous la régime de la *Loi sur la protection des renseignements personnels* adoptée par le Parlement. Ce modèle repose sur la nomination d'un haut fonctionnaire du Parlement, le commissaire à la protection de la vie privée, qui conseille le Parlement sur des questions en matière de vie privée, analyse les répercussions des initiatives en matière de législation et de réglementation de manière à ce que les membres du Parlement ainsi que les Canadiens et les Canadiennes soient en mesure de prendre des décisions éclairées, et agit comme ombudsman en vue de protéger les droits à la vie privée, et ce, en recourant à la négociation, à la persuasion et au dialogue, et parfois, en dernier ressort, à la publicité. Le système mis en place aux termes de la *Loi sur la protection des renseignements personnels* s'est rapidement révélé utile et nul n'a été surpris qu'il ait été approuvé et mis en application dans le secteur privé lorsque le Parlement a adopté la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Nous sommes confiants que, durant la dernière année, le Parlement a su tirer parti de ce système et que, à vrai dire, son utilité a été réaffirmée. Le Parlement a repensé et révisé des initiatives législatives, comme le projet de base de données de l'ADRC, pour réduire au minimum ses répercussions sur le droit à la vie privée. À notre avis, l'avenir du droit à la vie privée au Canada s'annonce bien malgré toutes les pressions subies.

L'année 2003 revêt une importance particulière en ce qui a trait à l'autre loi que nous administrons, la *Loi sur la protection des renseignements personnels et les documents électroniques* ou la *LPRPDÉ* comme nous l'appelons, en ce sens qu'il s'agit de la dernière année avant que cette loi ne soit totalement appliquée. En effet, cette loi est entrée en vigueur progressivement. Au départ, soit en 2001, elle s'appliquait à certains échanges de renseignements de nature commerciale, mais elle excluait les renseignements personnels sur la santé. À compter de janvier 2002, son application s'est élargie pour inclure les renseignements personnels sur la santé. L'étape finale débutera en janvier 2004, alors que la *Loi* s'appliquera à toute activité commerciale menée au Canada, sauf dans les provinces où une loi essentiellement similaire aura été adoptée. (Jusqu'à présent, seul le Québec dispose d'une loi sur la protection des renseignements personnels réputée être essentiellement similaire, mais la Colombie-Britannique et l'Alberta ont toutes deux déposé une loi cette année. Ce qui augure bien pour la protection du droit à la vie privée au Canada).

D'une manière générale, l'adoption et la mise en œuvre de la *Loi* se sont déroulées bien plus harmonieusement que certains l'avaient prévu. Le milieu des affaires a bien répondu aux exigences de conformité à la loi et, bien qu'il y ait eu quelques embûches sur la route, la nouvelle façon de faire des affaires n'avait pas été, dans l'ensemble, aussi difficile ou traumatisante qu'on l'avait craint. Nous observons un consensus général autour du fait que le respect du droit à la vie privée n'est pas une tâche aussi onéreuse que certaines personnes l'auraient cru, mais constitue simplement, en fait, une bonne pratique commerciale. Un des signes les plus encourageants réside dans l'intérêt manifeste des gens d'affaires à vouloir se conformer à la *Loi*. En fait, une sorte d'industrie artisanale de la conformité a vu le jour, constituée d'une multitude de sociétés d'experts-conseils offrant leur savoir-faire aux entreprises désireuses de se conformer à la *Loi*. Presque chaque semaine, nous recevons une brochure annonçant la tenue d'un séminaire ou d'un atelier traitant de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

De surcroît, le modèle de l'ombudsman, qui a fait ses preuves sous le régime de la *Loi sur la protection des renseignements personnels*, a également donné de

bons résultats en ce qui a trait à la *LPRPDÉ*. Nous avons été heureux de constater la volonté des organisations du secteur privé assujetties à la *Loi* de se conformer à ses exigences et de reconnaître l'expertise particulière du Commissariat pour traiter en profondeur les questions liées au droit à la vie privée.

Nous observons un consensus général autour du fait que le respect du droit à la vie privée n'est pas une tâche aussi onéreuse que certaines personnes l'auraient cru, mais constitue simplement, en fait, une bonne pratique commerciale.

Pour ce qui est des activités quotidiennes, le Commissariat a continué de relever des défis de taille, mais il demeure une organisation solide et performante face à la forte demande du public à l'égard de ses services. Nous avons traité un volume important de plaintes déposées en vertu de la *Loi sur la protection des renseignements personnels*, avec une hausse de 35 % de nouvelles plaintes cours de la dernière année. En ce qui a trait à la *LPRPDÉ*, le nombre de nouvelles plaintes a presque triplé au cours de la même période et nous pouvons nous attendre à ce que l'élargissement de l'application de la *Loi* en 2004 entraîne une augmentation considérable du nombre de plaintes.

Un fait nouveau ayant marqué la dernière année a trait à la présentation de la nouvelle politique du Conseil du Trésor sur les évaluations des facteurs relatifs à la vie privée.

Une évaluation des facteurs relatifs à la vie privée, ou une ÉFVP, vise simplement à déterminer comment et dans quelle mesure un programme ou une activité comporte des incidences sur le droit à la vie privée des citoyens. Généralement, l'ÉFVP comporte une description du programme, une analyse

de ce qu'il adviendra des renseignements personnels recueillis, utilisés et communiqués, ainsi qu'une évaluation de la conformité du programme avec les principes, la loi et les politiques liés à la protection des renseignements personnels. La nouvelle politique du Conseil du Trésor fait des ÉFVP une condition relativement au financement de tous les programmes et services qui sont nouveaux, considérablement modifiés ou offerts par voie électronique et qui requièrent la collecte, l'utilisation et la communication de renseignements personnels. Le Canada est le premier pays dans le monde à rendre les ÉFVP obligatoires en ce sens.

La mise en œuvre de cette politique implique que les institutions gouvernementales devront tenir compte du droit à la vie privée dès le départ, dès le moment où elles commenceront à planifier un nouveau programme. L'importance de cette démarche réside dans le fait qu'on cherchera à déterminer si un programme ou un projet a une incidence négative sur le droit à la vie privée — à savoir, par exemple, s'il prévoit un nouveau couplage de données ou davantage d'échanges de renseignements personnels, ou encore s'il entraîne le recours à de nouveaux identificateurs personnels communs ou une utilisation accrue de ceux qui existent déjà — avant qu'il n'y ait atteinte au droit à la vie privée. À l'égard d'un enjeu comme le droit à la vie privée, il est plus logique d'adopter une approche préventive comme celle-ci, plutôt qu'une approche punitive ou réparatrice. De fait, lorsqu'il y a atteinte au droit à la vie privée, lorsque des renseignements personnels concernant une personne ont été soustraits à son contrôle, il est trop tard. En matière de droit à la vie privée, ce qui est perdu ne peut être retrouvé. C'est pourquoi la politique du Conseil du Trésor est si bien accueillie. Lorsque des initiatives gouvernementales viennent renforcer une saine gouvernance, il faut en reconnaître la valeur et s'en féliciter.

L'année nous a donc apporté quelques bonnes nouvelles et quelques déceptions et de nombreux défis toujours à relever. Heureusement, nous n'avons pas eu à nous attaquer seuls à nos défis. En effet, la protection du droit à la vie privée nous amène à prendre part à un dialogue permanent, au Canada et à l'étranger, avec des défenseurs du droit de à la vie privée, des défenseurs des libertés civiles, des universitaires et, bien sûr, d'autres

commissaires à la protection de la vie privée et des données personnelles. Ces différents intervenants nous ont aidé à porter le fardeau des déceptions et on doit leur reconnaître tout le mérite qu'ils ont d'avoir fait leur part pour ce qui est des bonnes nouvelles.

L'année nous a donc apporté quelques bonnes nouvelles et quelques déceptions, et de nombreux défis toujours à relever.

Le Comité permanent des opérations gouvernementales a rempli son devoir en rendant le Commissariat imputable à l'égard de normes plus strictes en matière de prudence et de probité dans l'utilisation des fonds publics. Alors que nous débutons une autre année décisive en ce qui a trait aux enjeux touchant la vie privée, le Commissariat à la protection de la vie privée s'emploiera à obtenir l'appui renouvelé du Sénat et de la Chambre des communes en vue d'atténuer l'incidence des technologies et des politiques envahissantes, qui portent atteinte aux droits à la vie privée des Canadiens et des Canadiennes.

Lois provinciales essentiellement similaires

Aux termes de l'alinéa 26 (2)*b*) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, le gouverneur en conseil peut exclure une organisation, activité ou catégorie d'activités de l'application de la *LPRPDÉ* à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels, qui s'effectue à l'intérieur de la province qui a adopté une loi étant réputée être essentiellement similaire à la *LPRPDÉ*.

Le but de cette disposition est de permettre aux provinces et aux territoires de réglementer les pratiques de gestion des renseignements personnels des organisations faisant affaires à l'intérieur de leurs frontières, sous réserve qu'ils disposent d'une loi qui soit essentiellement similaire à la *LPRPDÉ*.

Si le gouverneur en conseil émet un décret déclarant qu'une loi provinciale est essentiellement similaire, la collecte, l'utilisation ou la communication de renseignements personnels par des organisations assujetties à la loi provinciale ne seront pas visées par la *LPRPDÉ*. Néanmoins, les renseignements personnels, qui seront communiqués à l'extérieur de cette province ou du pays seront assujettis à la *LPRPDÉ*, qui continuera également à s'appliquer, dans les limites d'une province, aux activités des installations, ouvrages entreprises et secteurs d'activité fédéraux qui relèvent de la

compétence fédérale, telles les opérations bancaires, la radiotélévision, les télécommunications et les transports.

Le 22 septembre 2001, le ministère de l'Industrie a publié un avis dans la partie I de la *Gazette du Canada* (22 septembre 2001) établissant le processus que le ministère utilisera pour déterminer si les lois provinciales ou territoriales sont réputées être essentiellement similaires.

Le processus sera enclenché par une province, un territoire ou une organisation avisant le ministre de l'Industrie de la loi qui, à son avis, est essentiellement similaire à la *LPRPDÉ*. Le ministre peut aussi agir de son propre chef et recommander au gouverneur en conseil de désigner une loi provinciale ou territoriale comme étant essentiellement similaire.

Le ministre a déclaré qu'il sollicitera le point de vue du commissaire à la protection de la vie privée en vue de déterminer si la législation est essentiellement similaire et il inclura le point de vue de ce dernier dans la soumission au gouverneur en conseil.

Le processus offre également une occasion au public et aux parties intéressées de commenter la législation dont il est question.

Selon l'avis publié dans la *Gazette du Canada*, le ministre s'attend à ce que les lois essentiellement similaires des provinces ou des territoires comportent ce qui suit :

- qu'elles intègrent les dix principes de l'annexe 1 de la *LPRPDÉ* ;
- qu'elles prévoient un mécanisme de surveillance et de recours indépendant et efficace comportant des pouvoirs d'enquête ;
- qu'elles restreignent la collecte, l'utilisation et la communication des renseignements personnels à des fins qui sont appropriées ou légitimes.

En plus de fournir des commentaires au ministre de l'Industrie relativement à la loi spécifique provinciale ou territoriale, le commissaire à la protection de la vie privée est tenu, aux termes du paragraphe 25 (1), de rendre compte

chaque année au Parlement du Canada de la « mesure dans laquelle les provinces ont édicté des lois essentiellement similaires à la *LPRPDÉ* ».

Le processus offre également une occasion au public et aux parties intéressées de commenter la législation dont il est question.

Le commissaire précédent a publié deux rapports au Parlement au sujet des lois provinciales essentiellement similaires. En mai 2002, il a publié un rapport dans lequel il a conclu que la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec est essentiellement similaire à la *LPRPDÉ* en ce qui a trait à la mesure dans laquelle elle protège les renseignements personnels. En juin 2003, le commissaire précédent a publié un second rapport dans lequel il a émis des réserves concernant les projets de loi 44 et 38, qui ont été présentés respectivement par les provinces de l'Alberta et de la Colombie-Britannique, mais qui n'ont pas encore été adoptés.

Étant donné qu'aucun de ces projets n'a été adopté, nous continuerons à surveiller leur évolution et maintenir un dialogue avec nos homologues provinciaux.

Partie I

Rapport concernant la *Loi sur la protection des renseignements personnels*

INTRODUCTION

La *Loi sur la protection des renseignements personnels*, qui est entrée en vigueur depuis 1983, assure la protection de la vie privée des personnes en ce qui concerne les renseignements personnels détenus par les institutions du gouvenement fédéral. La *Loi* régit la manière dont ces institutions recueillent, utilisent, communiquent des renseignements personnels, ainsi que la manière dont elles procèdent à leur retrait, et accorde aux personnes le droit de demander accès à leurs renseignements personnels et celui de demander que des corrections soient apportées. Elle établit en outre les fonctions, les responsabilités et le mandat du commissaire à la protection de la vie privée du Canada.

Le commissaire à la protection de la vie privée reçoit des plaintes de personnes qui estiment que leurs droits aux termes de la *Loi* ont été enfreints et fait enquête sur ces plaintes. Le commissaire peut également prendre l'initiative d'une plainte et faire enquête lui-même concernant toute situation pour laquelle il a des motifs raisonnables de croire que la *Loi* a été enfreinte.

En tant qu'ombudsman, la principale priorité du commissaire est de résoudre les plaintes autant que possible, par la médiation et la négociation au besoin. Mais le commissaire possède aussi de vastes pouvoirs d'enquête que lui

confère la *Loi* – il peut assigner des témoins à comparaître et à témoigner, pénétrer dans des locaux afin de se faire remettre des documents et mener des entrevues. L'entrave aux enquêtes constitue une infraction à la *Loi*. Bien que la *Loi* ne lui confère pas de pouvoirs de rendre des ordonnances, le commissaire peut, suivant les conclusions d'une enquête, recommander aux institutions fédérales de modifier la manière dont elles traitent les renseignements personnels.

En outre, le commissaire est investi du mandat de mener des vérifications périodiques des institutions fédérales et de recommander des changements aux pratiques qu'il juge non conformes à la *Loi*.

Aux termes de la *Loi*, le commissaire est tenu de déposer un rapport annuel au Parlement sur les activités de l'exercice précédent du Commissariat. Le présent rapport vise la période du 1er avril 2002 au 31 mars 2003 au titre de la *Loi sur la protection des renseignements personnels*.

ENQUÊTES ET DEMANDES DE RENSEIGNEMENTS

La Direction des enquêtes et des demandes de renseignements du Commissariat est chargée de mener des enquêtes sur les plaintes que déposent des personnes aux termes de l'article 29 de la *Loi sur la protection des renseignements personnels* (et aux termes de l'article 11 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, dont il sera question plus loin dans le rapport).

Ces enquêtes permettent, essentiellement, de déterminer si les droits à la vie privée des personnes ont été enfreints et si ces dernières ont pu avoir accès à leurs renseignements personnels.

Lorsque les droits à la vie privée et le droit d'accès ont été enfreints, le processus d'enquête cherche à trouver des voies de recours pour les personnes et à empêcher que les violations ne se reproduisent.

La *Loi sur la protection des renseignements personnels* autorise le commissaire à faire prêter serment, à recevoir des éléments de preuve, à pénétrer dans des locaux le cas échéant, à examiner ou à se faire remettre des exemplaires de documents trouvés dans n'importe quel local.

Nous sommes heureux de signaler que nous avons obtenu des collaborations volontaires jusqu'à présent et que toutes les plaintes adressées au commissaire ou à ses prédécesseurs ont été résolues sans que nous n'ayons à invoquer ces pouvoirs d'enquête officiels.

En outre, la Direction des enquêtes et des demandes de renseignements répond chaque année à des milliers de demandes provenant des particuliers et des organisations qui s'adressent au Commissariat afin d'obtenir des conseils et de l'aide pour toutes sortes de questions liées à la protection des renseignements personnels.

Enquêtes terminées sur des plaintes déposées
Du 1er avril 2002 au 31 mars 2003

En 2001-2002 :	1 673
En 2002-2003 :	3 483

PLAINTES EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Au cours de l'année sur laquelle porte le présent rapport, le Commissariat a reçu 1 642 nouvelles plaintes. Environ 43 % de ces nouvelles plaintes ont été déposées par des personnes alléguant que leur droit d'accès en vertu de la *Loi sur la protection des renseignements personnels* a été enfreint ; 24% concernaient des allégations selon lesquelles les dispositions en matière de confidentialité de la *Loi* en ce qui concerne la collecte, l'utilisation, la communications, la conservation et le retrait des renseignements personnels n'avaient pas été respectées ; les 33 % restants portaient sur la lenteur d'institutions gouvernementales à répondre à des demandes d'accès à des renseignements personnels.

Plus des deux tiers du total des plaintes reçues étaient à l'encontre de cinq institutions du gouvernement fédéral : le Service correctionnel du Canada, l'Agence des douanes et du revenu du Canada, la Gendarmerie royale du Canada, le ministère de la Défense nationale et Citoyenneté et Immigration Canada.

L'ancien commissaire a rendu des conclusions sur 3 483 plaintes au cours de l'année sur laquelle porte ce rapport. Il est important de noter que ce chiffre comprend 2 323 plaintes liées à la communication, par l'Agence des douanes et du revenu du Canada (ADRC), de renseignements personnels figurant sur les cartes de déclaration douanière E-311 à Développement des ressources humaines Canada (DRHC).

La question en litige portait sur l'autorité nécessaire pouvant justifier l'utilisation de renseignements personnels recueillis par l'ADRC à une fin donnée – pour la déclaration de biens qu'un voyageur apporte au Canada – en vue de l'emploi par DRHC à des fins tout autres, c'est-à-dire dans le cadre d'un programme de couplage de données d'enquête ayant pour but d'identifier les voyageurs de retour au pays qui recevaient frauduleusement des prestations d'assurance-emploi alors qu'ils se trouvaient à l'étranger.

L'affaire a été portée devant un tribunal afin de déterminer si la communication était autorisée en vertu du paragraphe 8(2)*b*) de la *Loi sur la protection des renseignements personnels* et de l'article 108 de la *Loi sur les douanes* et si l'utilisation de cette information par DRHC comme preuve contre ces personnes enfreignait leurs droits en vertu de la *Charte canadienne des droits et libertés*.

La Cour suprême du Canada a jugé que la communication était autorisée en fonction de ses interprétations de ces dispositions de la *Loi sur la protection des renseignements personnels* et de la *Loi sur les douanes*. Elle a aussi confirmé la décision du tribunal inférieur selon laquelle, en raison de la nature limitée des renseignements communiqués, il n'y avait aucune attente raisonnable quant à la protection des renseignements personnels, décision suivant laquelle, par conséquent, les voyageurs n'avaient pas été privés de leur droit, en vertu de la *Charte*, d'être protégés contre toute fouille ou saisie déraisonnable. Compte

tenu de ce fait, l'ancien commissaire était tenu d'informer les plaignants que leurs plaintes étaient non fondées.

Parmi les 1 160 autres plaintes résolues, 486 portaient sur des questions d'accès, 293 concernaient la collecte, l'utilisation, la communication, la conservation et le retrait de renseignements personnels et 381 concernaient les délais prescrits. Les conclusions relativement à ces 3 483 plaintes ont été rendues comme suit :

Non fondées :	2 711
Fondées :	371
Fondées et résolues :	77
Résolues :	13
Résolues en cours d'enquête :	235
Abandonnées :	76

DÉFINITION DE CONCLUSIONS AUX TERMES DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Non fondée : Lorsqu'une plainte est jugée *non fondée*, cela signifie que l'enquête n'a relevé aucun élément de preuve qui porte le commissaire à conclure que l'institution fédérale n'a pas respecté les droits d'un plaignant aux termes de la *Loi sur la protection des renseignements personnels*.

Fondée : Lorsqu'une plainte est jugée *fondée*, cela signifie que l'institution fédérale n'a pas respecté les droits d'une personne aux termes de la *Loi sur la protection des renseignements personnels*. Ce serait également la conclusion du commissaire dans une situation où l'institution fédérale refuse d'accorder l'accès à des renseignements personnels malgré notre recommandation qui veut que ceux-ci soient communiqués. En pareil cas, la prochaine étape pourrait consister à demander un recours en révision à la Cour fédérale du Canada.

Fondée et résolue : Le commissaire conclut qu'une plainte est *fondée et résolue* lorsque les allégations sont corroborées par l'enquête et que l'institution

fédérale a accepté volontairement de prendre des mesures correctives pour remédier à la situation.

Résolue : Il s'agit d'une conclusion officielle qui reflète le rôle d'ombudsman du commissaire. Cette conclusion est réservée aux plaintes pour lesquelles une conclusion *fondée* serait trop sévère dans les cas de mauvaise communication ou de malentendu. Cela signifie que le Commissariat, après avoir mené une enquête complète et minutieuse, a permis de négocier une solution qui satisfait toutes les parties.

Résolue en cours d'enquête : Il ne s'agit pas d'une conclusion officielle, mais d'une façon acceptable de résoudre une plainte. Une fois l'enquête terminée, le plaignant est satisfait des efforts déployés par le Commissariat et consent à laisser tomber l'affaire. Le plaignant retient toutefois le droit de demander qu'une conclusion officielle soit rendue. Le cas échéant, l'enquêteur rouvre le dossier et dépose un rapport officiel. Le commissaire fait alors rapport sur les conclusions dans une lettre au plaignant.

Abandonnée : Il s'agit d'une enquête qui est terminée avant que toutes les allégations ne soient pleinement examinées. Une affaire peut être *abandonnée* pour toutes sortes de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, qui sont essentiels pour en arriver à une conclusion. Le commissaire ne rend pas de conclusions officielles lorsqu'une plainte est abandonnée.

SOMMAIRE DE CAS CHOISIS EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

CIC recueillait des renseignements relatifs à l'impôt sur le revenu d'employeurs canadiens

Trois personnes qui souhaitaient employer des aides familiaux résidants des Philippines se sont plaintes au Commissariat du fait que l'ambassade canadienne à Manille leur a demandé de fournir des renseignements sensibles

relatifs à l'impôt sur le revenu comme condition préalable à la délivrance de visas à leurs aides familiaux éventuels. Les personnes s'inquiétaient du fait d'avoir à envoyer des documents d'impôt contenant leur numéro d'assurance sociale (NAS), ainsi que des renseignements détaillés sur leur situation financière dans un pays étranger, surtout à un moment où l'usurpation d'identité est devenue l'objet d'une si grande préoccupation.

Citoyenneté et Immigration Canada (CIC) a expliqué que le Programme concernant les aides familiaux résidants (PAFR) fait venir au Canada des aides familiaux qualifiés dans les situations où aucun Canadien ou résident permanent ne peut occuper certains postes. Les Canadiens qui souhaitent embaucher un aide familial de l'étranger sont tenus de faire valider leur offre d'emploi par l'entremise de Développement des ressources humaines Canada (DRHC) et de signer un formulaire déclarant qu'ils peuvent subvenir aux besoins de la personne qu'ils emploieront.

Après que l'offre d'emploi a été validée par DRHC, la section des visas de l'ambassade canadienne à Manille a demandé aux employeurs éventuels de lui envoyer leur avis de cotisation des deux dernières années, leurs bordereaux T-4 et une lettre de leur employeur confirmant leur emploi.

CIC a soutenu que l'information était nécessaire pour déterminer l'authenticité d'une offre d'emploi et pour confirmer que les employeurs étaient financièrement en mesure de subvenir aux besoins d'un aide familial.

Lorsqu'on a mis en question l'autorité de CIC de recueillir des renseignements concernant l'impôt sur le revenu dans le but de délivrer des visas à des tiers, CIC a fait référence à l'article 203 du *Règlement sur l'immigration et la protection des réfugiés*. Un examen de ce document a indiqué que l'agent des visas doit déterminer si l'offre d'emploi est authentique et si l'emploi du ressortissant étranger aura probablement des retombées économiques neutres ou positives sur le marché du travail au Canada.

Dans le rapport annuel de l'an dernier, l'ancien commissaire a énoncé son point de vue concernant la collecte, sans fondement légal, de renseignements

relatifs à l'impôt sur le revenu. Il a expliqué qu'à son avis il est inacceptable qu'on demande à des personnes de produire leurs déclarations de revenus à des fins autres que celles qui sont prévues par la loi. Les Canadiens et Canadiennes ne devraient jamais accepter qu'un de leurs droits fondamentaux soit brimé lorsqu'ils font affaire avec le gouvernement.

Le Commissariat a présenté ces arguments à CIC. En conséquence de quoi, l'ambassade à Manille nous a confirmé qu'elle avait cessé de demander des renseignements relatifs à l'impôt sur le revenu pour la délivrance de visas aux aides familiaux résidants.

Collecte par l'ADRC de renseignements médicaux aux fins de l'impôt sur le revenu

Nous avons reçu une plainte de la part d'une famille qui allègue que l'Agence des douanes et du revenu du Canada (ADRC) a recueilli de manière inappropriée des renseignements personnels à son sujet auprès d'un fournisseur d'assurance-maladie provincial. Cette famille s'est établie en Afrique pendant trois ans, et avant de quitter le Canada, le mari a consulté l'ADRC, qui l'a informé que, aux fins de l'impôt sur le revenu, il serait considéré comme personne non-résidente durant son séjour à l'étranger. Pourtant, de retour au Canada, il a appris qu'il ne satisfaisait pas aux critères de non-résidence et a donc été imposé en conséquence. Par la suite, après avoir présenté à l'ADRC une demande en vertu de la *Loi sur la protection des renseignements personnels*, il a appris que l'Agence avait demandé à son fournisseur d'assurance-maladie provincial de lui communiquer tous ses dossiers médicaux, ainsi que ceux de sa femme et de ses enfants, notamment des dossiers qui dataient de quelque huit mois avant leur départ pour l'Afrique, et d'autres de près de deux ans et demi après leur retour au Canada.

Nous avons établi qu'une personne ne peut être considérée comme non-résident aux fins de l'impôt que si l'ADRC juge qu'elle a suffisamment rompu ses liens avec le Canada après son déménagement dans un autre pays. L'ADRC s'appuie sur des dispositions de la *Loi de l'impôt sur le revenu* pour recueillir l'information nécessaire en vue de l'évaluation du statut de non-résident. Elle effectue couramment des enquêtes dans le cadre du processus d'évaluation du

statut des particuliers, notamment en vérifiant si ceux-ci continuent de réclamer des indemnités aux termes d'un régime d'assurance-maladie provincial pendant leur séjour à l'étranger. En effet, toute personne qui dépose de telles réclamations montre par là qu'elle n'a peut-être pas rompu tous ses liens avec le Canada.

L'ancien commissaire a déterminé que l'ADRC dispose de l'autorité nécessaire, en vertu de la *Loi de l'impôt sur le revenu*, pour recueillir auprès de sources provinciales des renseignements personnels sur tous les membres de la famille dans le but d'établir leur statut de non-résidence. Néanmoins, l'ancien commissaire avait des réserves quant à la *quantité* des renseignements médicaux recueillis, particulièrement en ce qui concerne les renseignements relatifs aux périodes de temps qui se sont écoulées avant et après le séjour de la famille en Afrique. Les responsables de l'ADRC ont convenu qu'il était excessif d'exiger des renseignements médicaux portant sur une période de deux ans et demi après le retour de la famille.

Dans les circonstances, l'ancien commissaire a conclu que l'ADRC avait recueilli plus de renseignements personnels que nécessaire et que, par conséquent, elle avait outrepassé le pouvoir que lui confère l'article 4 de la *Loi sur la protection des renseignements personnels*. Il a déterminé que les plaintes étaient fondées et recommandé que l'ADRC détruise les renseignements obtenus auprès de la province.

Communication par mégarde de renseignements médicaux sensibles par l'AIPRP

Les renseignements personnels sur la santé – ceux qui portent sur notre santé physique et mentale – constituent probablement les données les plus confidentielles qui soient. Lorsque de tels renseignements ne sont pas traités avec le plus grand soin et avec la plus stricte confidentialité, leur communication peut avoir des conséquences désastreuses. L'affaire suivante en est un bon exemple : une personne a présenté une demande en vertu de la *Loi sur l'accès à l'information* (LAI) à une institution gouvernementale visant l'ensemble des documents portant sur la nomination d'un autre employé du gouvernement à un poste donné. Les noms des deux parties ne présentaient

qu'une vague ressemblance. Pourtant, étant donné qu'il n'a pas pris soin de bien lire les noms des deux personnes, l'analyste du bureau d'accès à l'information et à la protection des renseignements personnels (AIPRP) du ministère a présumé que le requérant et l'employé nommé étaient la même personne. Par conséquent, presque tous les renseignements versés au dossier de dotation ont été communiqués au requérant — seule une petite partie de renseignements relatifs à une tierce personne a été retirée. Le dossier contenait non seulement l'adresse et le numéro de téléphone privés de l'employé nommé au poste, mais aussi des renseignements à caractère très personnel le concernant -- des renseignements très détaillés sur sa situation médicale et financière, des renseignements sur sa famille, sur ses antécédents en matière d'emploi, et des renseignements sur ses études. On a, par ailleurs, découvert que les deux individus avaient des rapports difficiles et que le requérant avait par la suite utilisé certains des renseignements médicaux obtenus afin de mener des enquêtes personnelles sur l'employé nommé au poste.

Lorsque de tels renseignements ne sont pas traités avec le plus grand soin et avec la plus stricte confidentialité, leur communication peut avoir des conséquences désastreuses.

Après enquête, l'institution a admis promptement son erreur, présenté ses excuses à l'employé et lui a remis une copie des mêmes documents envoyés au requérant, afin qu'il puisse savoir précisément quels renseignements à son sujet avaient été communiqués de manière inappropriée. L'institution a, par ailleurs, demandé au requérant de retourner l'information reçue et de n'en garder aucune copie. Les documents ont bien été renvoyés, mais on ne peut être certain qu'aucune copie n'en a été conservée. D'ailleurs, même si des garanties à cet égard pouvaient être obtenues, le mal est déjà fait, et le requérant a déjà communiqué des renseignements personnels de l'employé à d'autres personnes.

L'ancien commissaire a reconnu qu'une erreur humaine non sans négligence était à l'origine de ce problème, mais il était consterné par le fait qu'une telle erreur ait pu être commise, surtout par les personnes qui, au sein de l'institution concernée, sont censées être les spécialistes en poste de la protection des renseignements personnels. Si les renseignements personnels de l'employé avaient été traités avec le soin qu'ils méritent, cette grave violation du droit à la vie privée n'aurait jamais eu lieu.

Communication des antécédents criminels d'une personne aux membres de sa famille

Une personne a porté plainte auprès du Commissariat du fait qu'un employé du Service correctionnel du Canada (SCC) a communiqué des renseignements sur ses antécédents criminels à certains membres de sa famille (dont ses jeunes enfants, qui ignoraient tout du passé de leur père), ainsi qu'au grand public. Le plaignant, qui avait été emprisonné quelques années auparavant dans l'établissement fédéral où l'employé travaillait, a accusé ce dernier d'avoir communiqué de l'information confidentielle obtenue dans l'exercice de ses fonctions.

Le SCC a aussi été saisi d'une plainte à ce sujet, et il a mené sa propre enquête. Dès le début, le plaignant a soutenu fermement que l'employé du SCC a communiqué des renseignements personnels le concernant. Ce dernier a maintenu que ce n'est pas lui qui a fait les remarques en question, mais plutôt un ami qui était présent au moment de la communication, ami qu'il a refusé de nommer, tant au cours de notre enquête que lors de celle du SCC. Tous nos efforts en vue de découvrir l'identité de cet ami ont été vains. Néanmoins, compte tenu de tous les renseignements recueillis durant l'enquête, l'ancien commissaire était disposé à conclure que les droits garantis au plaignant aux termes de la *Loi sur la protection des renseignements personnels* avaient été enfreints en raison même des actes de l'employé. De fait, le SCC a déterminé que l'employé avait enfreint le code de discipline de l'institution, ainsi que les dispositions de la *Loi sur la protection des renseignements personnels*, et il l'a suspendu sans solde pendant 15 jours.

Avant de rendre sa décision finale dans cette affaire, l'ancien commissaire a mis en question les motifs pour lesquels le SCC avait conclu qu'une suspension de trois semaines était une mesure appropriée dans les circonstances. Ce fut à ce moment seulement que nous avons appris que de nouveaux faits avaient incité le SCC à revenir sur sa décision et à annuler la suspension. Conscient de la sanction disciplinaire infligée à l'employé, l'ami de ce dernier avait avoué que c'était bien lui – et non l'employé – qui avait communiqué les renseignements personnels concernant le plaignant. Bien qu'il ne fût pas pleinement convaincu de la crédibilité de l'ami – et qu'il eût des appréhensions à cet égard –, le SCC a décidé d'annuler la suspension.

À la lumière de cet aveu, nous avons mené d'autres interrogations, mais nous n'avons trouvé aucune raison d'accepter la version des faits soutenue par l'ami. Compte tenu des éléments de preuve que nous avons obtenus, l'ancien commissaire a conclu que c'est bien l'employé qui a communiqué les renseignements personnels concernant le plaignant et que son ami n'a probablement fait l'aveu que lorsqu'il est apparu que les répercussions pour l'employé seraient plus graves que prévu. L'ancien commissaire a donc déterminé que la plainte était fondée et demandé au SCC de réexaminer sa décision.

L'ancien commissaire a aussi signalé au SCC qu'il aurait dû aviser nos représentants que l'ami de l'employé avait finalement fait un aveu, après toutes les tentatives infructueuses du SCC et du Commissariat en vue de le retrouver. L'ancien commissaire a jugé qu'il s'agissait là d'un fait extrêmement important, qui a incité le SCC à revenir sur son jugement initial et qui aurait pu, bien évidemment, avoir une incidence directe sur sa décision. Le SCC savait que nous menions une enquête relativement aux allégations du plaignant et, selon l'ancien commissaire, il aurait dû informer immédiatement nos représentants de ce rebondissement. On a assuré l'ancien commissaire que cet oubli était un incident isolé qui ne se reproduira plus.

Même un dossier public devrait être protégé

Une personne reçoit une enveloppe par messager, qui lui est adressée, contenant les documents d'appel du Régime de pensions du Canada

(RPC) d'une autre personne. Il croit que cette autre personne a probablement reçu ses propres documents d'appel par erreur.

Notre enquête sur cette affaire a confirmé ces craintes. L'autre personne avait en effet reçu de DRHC les renseignements d'appel du plaignant. La confusion résultait d'un manque d'attention au moment où les documents ont été glissés dans les enveloppes avant leur envoi.

L'article 8 de la *Loi sur la protection des renseignements personnels* limite la manière dont les institutions gouvernementales peuvent communiquer des renseignements personnels. En substance, les institutions ne peuvent communiquer de renseignements personnels à des tiers sans le consentement de la personne concernée par les renseignements, à moins qu'un des cas de communication autorisée, énoncés au paragraphe 8(2) de la *Loi*, ne s'applique.

DRHC a expliqué que les renseignements concernant le plaignant qui avaient été communiqués se composaient de documents déposés à la Cour fédérale et faisaient ainsi partie d'un dossier public. Étant donné que le paragraphe 69(2) de la *Loi sur la protection des renseignements personnels* stipule que l'article 8 ne s'applique pas aux renseignements personnels auxquels le public a accès, DRHC a prétendu qu'il n'avait pas enfreint la *Loi* en envoyant par mégarde l'information aux mauvaises personnes.

L'ancien commissaire n'était pas d'accord, parce que les renseignements concernant le plaignant n'avaient pas été communiqués à partir d'un dossier public. Le fait qu'ils se trouvent dans un dossier public n'annule pas la communication par DRHC des renseignements concernant le plaignant à quelqu'un qui n'avait nullement besoin de le savoir. En se fondant sur ce fait, l'ancien commissaire a conclu que la plainte était fondée.

Par suite de la plainte, DRHC a présenté ses excuses aux personnes concernées, leur a envoyé de nouveau les renseignements qui avaient été mal acheminés et a révisé ses procédures d'envoi par la poste afin de minimiser les risques qu'un tel incident se reproduise.

Communication non autorisée d'un numéro d'assurance sociale (NAS)

Nous avons fait enquête sur une plainte d'une personne selon laquelle Développement des ressources humaines Canada (DRHC) a communiqué de manière inappropriée son NAS à un détective privé.

Le plaignant avait intenté une action en justice contre une compagnie d'assurance qu'il croyait avoir mal traité sa demande d'indemnité. Durant les procédures judiciaires, il a appris que la compagnie d'assurance avait engagé un détective privé pour examiner sa situation financière. Il a obtenu copie du rapport du détective et pris note de références à ses demandes de renseignements adressées à DRHC, de même que l'information qu'il avait reçue par la suite. Mécontent en raison d'un manque de volonté manifeste de DRHC de tenir compte de ses préoccupations concernant cette atteinte à sa vie privée, il s'est finalement adressé au Commissariat pour obtenir de l'aide.

Au cours de l'enquête sur la plainte contre DRHC, nous avons établi qu'un employé de DRHC avait consulté le dossier du plaignant dans le Registre d'assurance sociale au même moment où le détective privé avait soumis ses demandes de renseignements. Bien que le plaignant ait fait part de ses préoccupations à DRHC, le Ministère n'a pas poursuivi davantage la question jusqu'à ce que le plaignant signale son intention d'assigner des employés de DRHC à témoigner au tribunal dans le cadre de sa poursuite intentée contre la compagnie d'assurance. À ce moment, il a demandé copie du dossier d'enquête de DRHC concernant la communication de son NAS et de tout renseignement lié aux mesures prises par DRHC à cet égard. Ce ne fut qu'à ce stade – presque dix mois après que le plaigant avait fait part pour la première fois de ses préoccupations – que DRHC a décidé de faire une enquête interne afin de déterminer si son NAS pourrait avoir été compromis et comment il l'aurait été.

Il est apparu clairement, à partir des éléments de preuve obtenus durant notre enquête, que l'employé de DRHC avait obtenu l'accès au NAS de cette personne sans justification et l'avait communiqué au détective privé. Les preuves ont aussi indiqué la possibilité que l'employé avait d'avoir aussi accès

à une quarantaine d'autres dossiers de clients dans le Registre d'assurance sociale, pour lesquels il n'y avait aucun dossier connexe de DRHC qui aurait exigé que l'employé consulte leurs fichiers de NAS.

Mécontent en raison d'un manque manifeste de volonté de DRHC de tenir compte de ses préoccupations concernant cette atteinte à sa vie privée, il s'est finalement adressé au Commissariat pour obtenir de l'aide.

L'ancien commissaire était préoccupé du manque de conviction de DRHC relativement au traitement de la plainte de la personne à propos de la communication de son NAS lorsque le Ministère en avait été tout d'abord informé. Il n'a pris aucune mesure autre que de lui émettre un nouveau NAS, en dépit du fait que plusieurs fonctionnaires étaient au courant de l'incident longtemps avant qu'il n'ait porté plainte auprès du Commissariat. L'ancien commissaire était tout aussi préoccupé du fait que, malgré les capacités apparemment adéquates des systèmes, les gestionnaires de DRHC ne surveillent pas régulièrement le Registre d'assurance sociale pour relever les activités qui sont de nature suspecte ou qui ne peuvent autrement être justifiées comme faisant partie des fonctions d'un employé et pour traiter de cela.

L'ancien commissaire a conclu que DRHC était responsable de la communication inappropriée, par son employé, du NAS de la personne au détective privé et que le Ministère avait, par conséquent, enfreint les dispositions en matière de confidentialité de la *Loi sur la protection des renseignements personnels*.

En réponse à cette conclusion, DRHC a entrepris de limiter les dégâts autant que possible. Le sous-ministre a envoyé une lettre d'excuses au plaignant et a mis en place des mesures qui amélioreront substantiellement la sécurité des

renseignements personnels dans la base de données du Registre d'assurance sociale, et qui permettront de mieux surveiller l'accès des employés au Registre. Nous sommes confiants que ces mesures amélioreront la capacité de DRHC de protéger les renseignements personnels dont il est responsable et d'empêcher toute autre atteinte à la vie privée des clients.

DRHC a aussi décidé de soumettre la question à la Gendarmerie royale du Canada en vue d'une enquête criminelle – l'employé a finalement été congédié par DRHC pour l'infraction à la sécurité.

Un recenseur de Statistique Canada trouvé non responsable de la communication de renseignements personnels aux banques

Une personne a allégué que Statistique Canada avait vendu son nom et son adresse à des institutions financières qui lui ont alors envoyé du courrier non sollicité. Cette personne voyageait fréquemment pendant de longues périodes de temps et avait une boîte postale. Elle séjournait dans un parc de véhicules de plaisance au moment du recensement de 2001 et le recenseur lui a expliqué qu'elle devrait utiliser l'adresse du parc pour les besoins du recensement, ce qu'elle a fait. Deux ou trois mois plus tard, elle a commencé à recevoir du courrier non sollicité qui lui était adressé au parc. Étant donné qu'elle avait uniquement utilisé cette adresse pour le recensement, il lui semblait logique que Statistique Canada devait avoir vendu ou sinon fourni l'adresse aux institutions financières.

Nous avons examiné une sollicitation qu'avait reçue cette personne et communiqué avec la banque qui la lui avait envoyée. Au moyen du code inscrit sur la lettre type, la banque a été en mesure de déterminer qu'elle avait obtenu son nom et son adresse au parc de l'une des plus grandes entreprises de gestion de listes au Canada, qui s'occupe de plus de 500 listes de publipostage contenant quelque 25 millions de noms. Ses représentants ont confirmé que les renseignements concernant la plaignante étaient contenus dans une des listes de publipostage créée et mise à jour à partir d'information obtenue de compagnies de téléphone provinciales au Canada.

Ce renseignement a permis à la personne de se rappeler qu'elle avait fait installer un téléphone au parc. Bien que sa facture téléphonique soit envoyée à sa boîte postale, elle avait dû fournir à la compagnie de téléphone l'adresse du parc pour l'installation et l'entretien de la ligne téléphonique. Il est devenu évident, dès lors, que c'était la compagnie de téléphone et non Statistique Canada qui avait communiqué les nom et adresse de la personne au commissionnaire en publipostage qui, à son tour, avait fourni les renseignements la concernant aux banques.

Au cours de l'enquête, on a demandé au commissionnaire en publipostage de retirer le nom de la personne de la liste de publipostage, ce qu'il a fait immédiatement. Toutefois, la personne a été informée de la possibilité que, bien que son nom ne se trouve plus sur une liste mise à jour, les anciennes listes que détenaient les clients du commissionnaire en publipostage pourraient toujours contenir les renseignements la concernant et par conséquent elle pourrait continuer de recevoir des sollicitations. L'ancien commissaire l'a exhortée à communiquer directement avec ces compagnies afin de faire retirer son nom de ces listes. Il lui ai aussi rappelé que son nom pourrait figurer sur d'autres listes à l'avenir si, par exemple, elle faisait une demande de carte de crédit, remplissait un bulletin de participation à un concours ou s'abonnait à des magazines.

Plaintes relatives aux délais de réponse

En vertu de la *Loi sur la protection des renseignements personnels*, les Canadiens et Canadiennes ont le droit d'avoir accès aux renseignements personnels les concernant que détiennent les institutions gouvernementales et, en vertu de la *Loi*, celles-ci doivent répondre dans les 30 jours suivant la réception de la demande. Toutefois, elles peuvent proroger ce délai d'une période maximale de 30 jours, mais seulement dans deux cas précis : le cas où le respect de la période de 30 jours entraverait de façon déraisonnable le fonctionnement de l'institution et le cas où des consultations s'avèrent nécessaires et rendraient pratiquement impossible l'observation de ce délai.

Le nombre de plaintes relatives aux institutions fédérales qui ne répondent pas dans les délais prescrits aux demandes d'accès aux renseignements

personnels des citoyens s'élevait à 541 cette année, en comparaison des 428 plaintes signalées au cours de l'exercice antérieur. Nous avons résolu 381 de ces plaintes, dont 302 étaient fondées.

Plus de plaintes ont été déposées au sujet des pratiques de traitement des renseignements personnels du Service correctionnel du Canada (SCC) que de toute autre institution du gouvernement fédéral. Parmi les 177 plaintes à l'encontre du SCC que le Commissariat a résolues, 159 étaient fondées. Bien que le SCC ait accru son effectif et rationalisé ses procédures, il continue de ne pas répondre aux demandes de renseignements personnels en temps opportun.

Le nombre de plaintes relatives aux délais de réponse de deux institutions ont considérablement diminué par rapport à l'an dernier, tandis que celles concernant quatre autres institutions ont augmenté, à savoir :

Agence des douanes et du revenu du Canada :	baisse de 85 à 31 plaintes ;
Développement des ressources humaines Canada :	baisse de 57 à 16 plaintes ;
Service correctionnel du Canada :	hausse de 125 à 233 plaintes ;
Gendarmerie royale du Canada :	hausse de 16 à 71 plaintes ;
Ministère de la Défense nationale :	hausse de 35 à 58 plaintes ;
Citoyenneté et Immigration Canada :	hausse de 40 à 49 plaintes.

Un élément qui continue de nuire à la capacité des institutions de répondre aux demandes dans les délais prescrits est la complexité du traitement des bandes sonores et des bandes vidéo.

Les institutions enregistrent parfois les entrevues menées dans le cadre d'enquêtes administratives ou criminelles. Étant donné que la *Loi sur la protection des renseignements personnels* s'applique aux renseignements personnels « quels que soient leur forme et leur support », les personnes peuvent demander copie de leurs renseignements sur ces bandes. Il s'agit d'un processus qui prend beaucoup de temps ; il faut écouter ou regarder les bandes, puis déterminer et retirer l'information qui, parce qu'elle contient

souvent des renseignements personnels concernant d'autres personnes, ne peut être communiquée aux requérants. Le ministère de la Défense nationale est un des organismes qui enregistre les entrevues. Il a récemment fait l'acquisition d'un nouvel équipement dans le but de tenter de simplifier le processus d'examen et de retrait de l'information sur bande.

Les demandes de dossiers d'enquête volumineux expliquent aussi certains retards et difficultés à répondre en temps opportun.

Transmission de renseignements par télécopieur

Bien que nous déconseillions aux institutions d'envoyer des renseignements personnels par télécopieur, nous nous rendons compte qu'elles utilisent régulièrement ce mode de transmission afin d'accélérer la réception de l'information.

Une de nos enquêtes a décelé un problème en ce qui concerne la façon dont une institution gouvernementale gardait un dossier contenant des renseignements personnels envoyés par télécopieur. Les pages couvertures de transmission par télécopieur indiquaient le nombre de pages envoyées, les noms du destinataire et de l'expéditeur, ainsi que la date, mais l'institution ne pouvait déterminer après coup quels documents ou pages en particulier avaient été transmis. Dans d'autres cas, l'institution ne pouvait préciser ce qui avait été reçu par télécopieur d'autres secteurs de l'institution.

Il est impératif que les institutions tiennent un relevé de l'utilisation et de la communication de renseignements personnels qui relèvent d'elles. Sauf dans un nombre limité de cas, les personnes ont le droit de savoir quels documents contenant leurs renseignements personnels sont envoyés, à qui ils sont envoyés et la raison pour laquelle ils sont communiqués.

Une solution à ce problème est de dresser une liste des documents envoyés ou reçus sur la page couverture même de transmission. Cela assurera la transparence, permettra de documenter la circulation de l'information et nous aidera dans nos enquêtes.

Traitement de dossiers originaux au lieu de photocopies

Certaines institutions gouvernementales ont refusé à des personnes l'accès à leurs renseignements personnels, contribuant ainsi à l'augmentation du nombre de plaintes adressées au Commissariat, eu égard au fait que les bureaux de l'accès à l'information et de la protection des renseignements personnels (AIPRP) au sein des ministères comptent de plus en plus sur des photocopies que leurs fournissent leurs secteurs de programme, plutôt que de travailler avec des documents originaux, lorsqu'ils traitent les demandes. Le problème que cela pose est que les analystes de l'AIPRP ne peuvent être certains que ce qu'on leur donne constitue tous les renseignements que souhaite obtenir une personne.

Lorsque le Commissariat reçoit une plainte concernant un « refus d'accès », il demande de voir le dossier original afin de le comparer à l'information traitée au bureau de l'AIPRP. Nous avons souvent constaté que le bureau de l'AIPRP ne disposait pas de tous les renseignements contenus dans le dossier original, parce que quelqu'un avait pensé qu'ils n'étaient pas pertinents ou avait enlevé les notes internes, ou simplement parce qu'on avait oublié le verso de documents recto-verso pendant la photocopie.

Les nuances subtiles qui ne peuvent être appréciées que lorsqu'on regarde un dossier original sont aussi perdues. Les photocopies ne reflètent pas l'utilisation ou la signification de formulaires de différentes couleurs ni n'indiquent la mise en relief de passages importants et peuvent ne pas saisir l'emplacement exact des notes avec commentaires sur papillons adhésifs. Elles ne contiennent pas non plus les trombones qui expliquent pourquoi certains documents sont groupés ensemble ou ne figurent pas dans l'ordre chronologique. Ces éléments sont essentiels pour comprendre le contexte du dossier et déterminer si les renseignements personnels peuvent être fournis à la personne.

L'examen, par nos enquêteurs, des dossiers originaux permet de lever tout doute concernant le fait que l'institution pourrait ne pas avoir trouvé tous les renseignements demandés et nous donne aussi la certitude sans équivoque dont nous avons besoin pour nous assurer que l'accès n'a pas été refusé.

Bien que certains secteurs de programme préfèrent ne pas remettre leurs dossiers originaux, tout particulièrement ceux qui concernent des activités administratives en cours, nous leur suggérons d'en garder une photocopie qu'ils peuvent utiliser durant les quelques jours pendant lesquels le bureau de l'AIPRP examine le dossier original. Nous exhortons également les coordonateurs de l'AIPRP à reprendre leur responsabilité pour la qualité des réponses qu'ils donnent aux personnes en travaillant uniquement avec des dossiers originaux.

INCIDENTS VISÉS PAR LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Il arrive parfois qu'on attire notre attention sur des incidents de mauvaise gestion de renseignements personnels pour lesquels un examen plus poussé du Commissariat est justifié. L'an dernier, nous avons effectué 32 examens de ce genre.

Par exemple, l'été dernier, après le déménagement d'un bureau d'un immeuble à un autre à Ottawa, le personnel de la Direction générale des prestations d'invalidité et des appels de Développement des ressources humaines Canada (DRHC) s'est rendu compte qu'il manquait deux ordinateurs. Bien qu'à la suite d'une enquête menée par sa Division de sécurité DRHC ne fût pas en mesure de déterminer exactement ce qui s'était produit, on croit que les ordinateurs ont été volés alors qu'ils avaient été laissés sans surveillance en attendant d'être chargés dans les fourgons de déménagement. On a suggéré qu'étant donné que les deux ordinateurs étaient neufs, on les avait pris en raison de leur valeur pécuniaire et non de leur contenu. Le vol a aussi été signalé au service de police local, qui n'a pas non plus été en mesure de trouver les ordinateurs manquants ni les auteurs du méfait.

Nos enquêteurs ont établi que les ordinateurs n'avaient pas été empaquetés dans des boîtes en carton, mais simplement placés sur des chariots sans être protégés d'aucune façon. Ils ont aussi établi qu'un employé de DRHC devait

s'assurer que tous les articles étaient transférés de leur emplacement original au point de chargement, mais que personne n'avait en fait supervisé le transfert de ces articles de cet emplacement à l'endroit où étaient stationnés les fourgons de déménagement à l'extérieur de l'immeuble.

Bien que les ordinateurs n'aient jamais été trouvés, DRHC a été en mesure de déterminer, au moyen de bandes de sauvegarde, qu'ils contenaient les nom et prénom complets, les numéros d'assurance sociale (NAS) et les renseignements médicaux de douzaines de bénéficiaires de prestations d'invalidité du Régime de pensions du Canada (RPC). Par conséquent, DRHC a décidé d'informer ces bénéficiaires du vol.

Durant notre examen de l'incident, nous avons toutefois remarqué que 38 autres personnes dont les noms de famille et NAS figuraient sur des documents n'avaient pas été informées. Étant donné qu'il s'agirait de renseignements personnels suffisants pour peut-être identifier ces personnes, nous avons demandé à DRHC de les informer aussi du vol, ce que le Ministère a fait.

Nous avons aussi recommandé que DRHC établisse des mesures de sécurité supplémentaires pour éviter qu'un tel incident ne se reproduise, plus particulièrement qu'il s'assure de retirer tous les renseignements personnels des lecteurs de disque dur des ordinateurs avant leur déménagement d'un endroit à un autre et de disposer de personnel supplémentaire présent lors des déménagements afin d'offrir une sécurité adéquate en ce qui concerne tout renseignement personnel touché par le déménagement.

Dans un autre incident, une personne a informé le Commissariat que des documents, qu'elle avait reçus de la cour des petites créances à propos des poursuites qu'elle avait intentées contre une autorité portuaire, contenaient des renseignements personnels relatifs à d'autres personnes, en particulier leurs numéros de compte de carte de crédit.

Notre personnel a établi que lorsque l'autorité portuaire avait déposé sa défense à la cour des petites créances, elle avait inclus copie d'un sommaire

journalier des recettes et des dépôts et un récépissé des dépôts en espèces. Ces documents identifiaient d'autres personnes et fournissaient leurs numéros de compte, numéros de facture, numéros de carte de crédit et les sommes payées à l'autorité portuaire.

Pour sa défense, l'autorité portuaire croyait n'avoir aucun autre choix que de déposer des documents complets et non révisés avec sa défense pour se conformer au déroulement de l'instance. Dans le cadre de sa défense, elle devait présenter l'information relative à ses opérations financières avec le plaignant et avait l'impression qu'elle ne pouvait retirer aucun renseignement concernant les autres personnes nommées dans ces documents.

Lorsque le Commissariat s'est informé auprès de la cour des petites créances, nous avons appris qu'elle accepterait en fait des documents partiels ou dont des portions ont été retirées. Par conséquent, l'autorité portuaire aurait pu retirer tous les renseignements qui ne concernaient pas le plaignant, dont les renseignements personnels relatifs à d'autres personnes, lorsqu'elle a déposé ses documents au tribunal. Nous avons attiré l'attention de l'autorité portuaire sur cette question et, en conséquence, elle a entrepris de retirer du dossier du tribunal les renseignements concernant les autres personnes. L'autorité portuaire a aussi communiqué avec les personnes concernées pour les informer que leurs renseignements personnels avaient été inclus dans un dossier public.

COMMUNICATIONS DANS L'INTÉRÊT PUBLIC

L'alinéa 8(2)*m)* de la *Loi sur la protection des renseignements personnels* autorise le responsable d'une institution gouvernementale à communiquer des renseignements personnels à l'insu et sans le consentement d'une personne concernée dans les cas où un intérêt public clairement prédominant l'emporte sur le droit à la vie privée de la personne ou la personne concernée en tirerait un avantage certain. En vertu du paragraphe 8(5) de la *Loi*, le commissaire à la protection de la vie privée doit être avisé d'avance de toute communication envisagée dans ce cadre.

L'année dernière, l'ancien commissaire a rappelé à deux ou trois institutions, après avoir examiné leur avis, que la latitude de communiquer des renseignements personnels dans l'intérêt public devrait être réservée aux cas exceptionnels, lorsque la communication ne peut être justifiée en vertu d'aucune autre disposition qui l'autorise dans la *Loi*.

Il était devenu de plus en plus évident que certaines institutions utilisaient la disposition de façon systématique et courante sans trop penser, à ce qu'il semble, à l'existence d'un intérêt public prédominant à ce moment. Cela était troublant, parce que la situation semblait peu ou pas du tout entrer en ligne de compte dans le processus décisionnel. Souvent, il n'y a eu aucune évaluation pour déterminer ce qui était d'intérêt public et si cet intérêt devrait l'emporter sur les droits à la vie privée de la personne. Étant donné qu'une personne n'a que rarement, sinon jamais, l'occasion de mettre en question la décision, il est essentiel que les décideurs agissent de façon judicieuse et s'assurent de disposer de tous les renseignements pertinents avant de prendre une décision équitable.

Toutefois, parmi les 70 avis de communication de renseignements personnels dans l'intérêt public que nous avons reçus durant l'année, un d'eux était clairement justifié : la décision du ministère de la Défense nationale (MDN) de communiquer au ministère des Anciens Combattants des renseignements concernant quelque 2 500 personnes impliquées dans des expériences de guerre chimique.

Depuis la Seconde Guerre mondiale jusqu'en 1992, Recherche et développement pour la défense Canada (RDDC), une direction générale du MDN anciennement connue sous le nom de Centre de recherches pour la défense, a dressé une liste des membres du MDN qu'elle avait exposés à divers produits chimiques dans le cadre de son programme de recherche sur la guerre chimique. Les membres étaient des volontaires, mais certains d'entre eux n'étaient peut-être pas conscients de leur participation aux expériences.

À la suite d'une récente enquête menée par le Bureau de l'ombudsman de la Défense nationale, le MDN croyait que les renseignements de RDDC aideraient le ministère des Anciens Combattants à identifier les anciens combattants qui pourraient avoir droit à des prestations. Les renseignements comprenaient le nom de famille et les initiales de la personne, le nom du produit chimique administré, la date et le lieu de l'administration. On y trouvait aussi quelques numéros matricules mais aucune date de naissance, ce qui rendait impossible pour le MDN d'établir effectivement une correspondance entre toutes les personnes et ses dossiers du personnel.

RDDC n'avait pas copié ces renseignements dans les états de service ou dossiers médicaux des employés touchés et le MDN espérait que le ministère des Anciens Combattants allait comparer l'information avec ses dossiers afin d'identifier toute correspondance dans son répertoire et communiquer avec les personnes en question. Le but en était que le ministère des Anciens Combattants puisse examiner les cas des anciens combattants qui déclaraient avoir été exposés à des produits nocifs, dont le charbon, mais auxquels on avait refusé toute aide financière parce qu'aucune preuve dans leurs états de service ou dossier médical ne permettait d'appuyer leurs revendications.

L'ancien commissaire a accepté volontiers la décision du MDN. Les avantages pour les personnes étaient évidents ; le ministère des Anciens Combattants pourrait aider à résoudre les questions relatives à l'admissibilité aux prestations en plus d'apporter son aide dans le diagnostic et le traitement des maladies causées par l'exposition aux substances toxiques.

Les dix premiers ministères selon le nombre de plaintes reçues

1er avril 2002 – 31 mars 2003

Organisation	Total	Accès aux renseignements personnels	Délais	Atteinte à la vie privée	Autre
Service correctionnel Canada	456	106	233	117	0
Agence des douanes et du revenu du Canada	205	127	31	47	0
Gendarmerie royale du Canada	200	101	71	28	0
Défense nationale	130	51	58	21	0
Citoyenneté et Immigration Canada	107	52	49	6	0
Développement des ressources humaines Canada	85	38	16	31	0
Société canadienne des postes	71	37	13	21	0
Ministère de la Justice Canada	65	47	13	5	0
Centre canadien du renseignement de sécurité	57	48	8	1	0
Commission canadienne de sûreté nucléaire	36	1	0	35	0
Autres	230	100	50	80	0
Total	**1 642**	**708**	**542**	**392**	**0**

Enquêtes terminées et résultats selon le ministère ou l'organisme

1er avril 2002 – 31 mars 2003

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Agriculture et Agroalimentaire Canada	2	1	1	2	0	5	**11**
Agence des douanes et du revenu du Canada	37	14	878	6	8	46	**989**
Société canadienne d'hypothèques et de logement	0	0	0	0	0	2	**2**
Société canadienne des postes	17	4	11	6	0	8	**46**
Patrimoine canadien	0	0	1	0	0	0	**1**
Commission canadienne des droits de la personne	0	0	1	0	0	0	**1**
Agence canadienne de développement international	1	0	1	0	0	0	**2**
Commission canadienne de sûreté nucléaire	0	0	35	1	0	0	**36**
Centre canadien du renseignement de sécurité	5	2	18	0	1	0	**26**
Agence spatiale canadienne	2	0	0	0	0	0	**2**
Citoyenneté et Immigration Canada	33	4	28	13	0	28	**106**
Commission des plaintes du public contre la GRC	0	0	5	0	0	0	**5**

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)

1er avril 2002 – 31 mars 2003

Organisation	Fondée	Fondée et résolue	Non fondée	Aban-donnée	Résolue	Résolue en cours d'enquête	Total
Service correctionnel Canada	189	17	42	11	1	65	325
Environnement Canada	0	1	2	3	0	0	6
Financement agricole Canada	1	0	0	0	0	1	2
Ministère des Finances Canada	0	1	0	0	0	0	1
Pêches et Océans Canada	1	3	4	1	0	0	9
Ministère des Affaires étrangères et Commerce international	0	0	5	0	0	0	5
Office de commercialisation du poisson d'eau douce	0	1	0	0	0	0	1
Santé Canada	2	1	6	1	0	1	11
Développement des ressources humaines Canada	19	7	1 568	6	2	6	1 608
Commission de l'immigration et du statut de réfugié	4	4	13	0	0	1	22
Affaires indiennes et du Nord Canada	1	0	2	0	0	3	6
Industrie Canada	0	0	1	0	0	1	2
Bureau de l'Inspecteur général du SCRS	0	0	2	0	0	0	2

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)
1er avril 2002 – 31 mars 2003

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Ministère de la Justice Canada	4	1	11	1	0	7	24
Archives nationales du Canada	1	0	1	1	0	3	6
Défense nationale	25	7	10	7	1	14	64
Commission nationale des libérations conditionnelles	0	0	1	1	0	3	5
Bureau du directeur général des élections	0	0	0	1	0	0	1
Commissariat aux langues officielles	0	1	0	0	0	1	2
Bureau du Conseil privé	0	1	5	0	0	0	6
Commission de la fonction publique du Canada	1	0	2	0	0	1	4
Travaux publics et Services gouvernementaux Canada	3	0	0	0	0	3	6
Gendarmerie royale du Canada	20	5	41	12	0	28	106
Solliciteur général Canada	0	0	6	0	0	0	6
Statistique Canada	0	0	6	0	0	6	12
Transports Canada	1	2	0	2	0	1	6
Secrétariat du Conseil du Trésor du Canada	0	0	2	0	0	0	2

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)

1er avril 2002 – 31 mars 2003

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Société du port de Vancouver	0	0	0	1	0	0	1
Anciens Combattants Canada	2	0	2	0	0	1	5
Total	**371**	**77**	**2 711**	**76**	**13**	**235**	**3 483**

Enquêtes terminées selon les motifs et les résultats

1er avril 2002 – 31 mars 2003

	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Accès aux renseignements personnels	14	72	228	36	5	131	**486**
Accès	14	71	221	33	5	129	**473**
Correction – annotation	0	1	7	3	0	0	**11**
Langue	0	0	0	0	0	2	**2**
Frais inexacts	0	0	0	0	0	0	**0**
Atteinte à la vie privée	56	4	2 445	17	8	86	**2 616**
Collecte	7	2	831	2	7	19	**868**
Conservation et retrait	4	0	4	0	0	13	**21**
Utilisation et communication	45	2	1 610	15	1	54	**1 727**
Délais	301	1	38	23	0	18	**381**
Corrections – délais	2	0	0	0	0	0	**2**
Délais	287	1	29	23	0	18	**358**
Avis de prorogation	12	0	9	0	0	0	**21**
Autre	0	0	0	0	0	0	**0**
Total	**371**	**77**	**2 711**	**76**	**13**	**235**	**3 483**

Lieu d'origine des enquêtes terminées

1er avril 2002 – 31 mars 2003

Province / Territoire	Nombre
Terre-Neuve	14
Île-du-Prince-Édouard	3
Nouvelle-Écosse	59
Nouveau-Brunswick	52
Québec	2 247
Région de la capitale nationale – Québec	22
Région de la capitale nationale – Ontario	96
Ontario	396
Manitoba	83
Saskatchewan	55
Alberta	167
Colombie-Britannique	273
Nunavut	0
Territoires du Nord-Ouest	0
Yukon	4
Étranger	12
Total	**3 483**

Demandes de renseignements en vertu de la *Loi sur les renseignements personnels*

1er avril 2002 au 31 mars 2003 : 5 183

Nous tenterons d'apporter des données détaillées au sujet de ces demandes de renseignements dans nos prochains rapports annuels.

EXAMENS ET PRATIQUES EN MATIÈRE DE VIE PRIVÉE

L'article 37 de la *Loi sur la protection des renseignements personnels* habilite le commissaire à entreprendre des examens de conformité des politiques et des pratiques de gestion des renseignements personnels des institutions fédérales. Cela signifie que le commissaire a la latitude de procéder à des vérifications pour déterminer si elles se conforment aux pratiques équitables en matière de traitement de l'information énoncées aux articles 4 à 8 de la *Loi*. La Direction des examens et des pratiques en matière de vie privée peut évaluer la conformité des organisations aux exigences de la *Loi sur la protection des renseignements personnels*.

Au lendemain du 11 septembre 2001, un certain nombre de ministères et d'organismes fédéraux ont reçu des augmentations considérables de fonds qui leur ont été alloués afin de leur permettre de mettre en œuvre des changements en vue de lutter contre le terrorisme et d'accroître la sécurité nationale. Afin d'évaluer l'incidence de ces mesures antiterroristes sur le droit à la vie privée des personnes, le Commissariat a amorcé cette année des examens des pratiques de traitement des renseignements personnels à la Gendarmerie royale du Canada, au Service canadien du renseignement de sécurité et au Centre de la sécurité des télécommunications. Ces examens seront terminés au cours du prochain exercice.

Un certain nombre de programmes et d'activités établis par des institutions et des organismes du gouvernement fédéral prévoient la communication de renseignements personnels au sujet de citoyens et de résidants canadiens à des départements et organismes du gouvernement des États-Unis. Au cours de cet exercice, le Commissariat a entamé un examen des accords, des ententes et des protocoles d'entente conclus entre le Canada et les États-Unis qui prévoient des dispositions pour la communication de renseignements personnels. Dix-huit ministères, départements et organismes ont été sélectionnés pour cet examen, qui sera terminé au cours du prochain exercice.

Outre les examens et les vérifications, le Commissariat conseille les organismes fédéraux sur les questions de conformité et les implications en

matière de droit à la vie privée de pratiques et de programmes actuels et nouveaux. La Direction des examens et des pratiques en matière de vie privée du Commissariat a participé à de nombreux efforts consultatifs avec les ministères, notamment le Secrétariat du Conseil du Trésor, Élections Canada, Statistique Canada, Développement des ressources humaines Canada, Affaires indiennes et du Nord Canada et Santé Canada.

Ces consultations concernent souvent l'examen de nouvelles propositions relatives à la gestion des renseignements, telles que les initiatives relatives au couplage des données, la création de bases de données et les ententes de partage de renseignements avec d'autres organisations. Il est important de noter que le rôle du commissaire demeure consultatif en ce qui a trait à de telles questions. Le commissaire ne donne, en aucun cas, l'approbation officielle de telles initiatives, ce qui pourrait compromettre son impartialité lors d'enquêtes ou d'examens ultérieurs.

Comme nous l'avons décrit dans nos rapports antérieurs, DRHC a établi un processus d'examen pour traiter des activités d'analyse, de recherche et d'évaluation de politiques qui comportent la connexion de banques de données distinctes. Une partie de ce processus comprend la consultation avec le Commissariat. Au cours de la dernière année, le Commissariat a analysé et commenté près d'une douzaine de présentations de DRHC, dont l'évaluation de l'option Travail partagé de DRHC, l'évaluation des Services d'information sur le marché du travail, l'évaluation des besoins du Programme canadien de prêts aux étudiants et le projet d'ensembles de données relativement au versement de prêt.

Un projet que le Ministère a envoyé au Commissariat, le système d'activités de l'employeur et de l'industrie, a été soumis comme projet concernant les connexions de banques de données. Après examen, le Commissariat a conclu que le projet exigeait plus que la simple connexion des banques de données existantes. Il entraînerait plutôt la création d'une nouvelle banque de données qui serait utilisée de façon continue. On n'a jamais envisagé de traiter de ce genre de projet à travers un tel processus. Par conséquent, nous avons informé DRHC qu'on traiterait de la question de façon plus appropriée

au moyen d'une évaluation des facteurs relatifs à la vie privée (ÉFVP), qui exige un examen plus rigoureux. Nous abordons de façon plus détaillée les évaluations des facteurs relatifs à la vie privée dans la section suivante de ce rapport.

Nous avons régulièrement remarqué une amélioration dans le détail et l'intégralité des présentations de DRHC à propos des questions relatives aux droits à la vie privée. Dans notre dernier rapport, nous avons exprimé des réserves concernant le fait que DRHC a communiqué des renseignements restreints relativement à des marchés passés avec des parties de l'extérieur et nous avons affirmé que DRHC devrait renforcer l'obligation contractuelle de ces parties afin de protéger le caractère privé des renseignements personnels durant leur administration temporaire. Bien que certaines des présentations que nous avons reçues ne répondent pas pleinement à nos attentes, le Ministère a réalisé des progrès en ce qui concerne ce problème au cours de la dernière année.

ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

Le 2 mai 2002, le Secrétariat du Conseil du Trésor du Canada a rendu publique une nouvelle directive exigeant que les ministères et organismes du gouvernement fédéral entreprennent une évaluation des facteurs relatifs à la vie privée (ÉFVP) pour tous les nouveaux programmes ou services qui soulèvent des questions liées au droit à la vie privée. Le Canada est le premier pays dans le monde qui rend obligatoires des ÉFVP dans tous les ministères et organismes fédéraux.

Pendant plus d'un an avant cette date, le Commissariat avait exhorté le gouvernement à adopter une politique sur l'ÉFVP, afin de s'assurer que les considérations relatives au droit à la vie privée sont intégrées aux projets dès le départ et non après coup. Nous avons félicité le gouvernement d'avoir mis en application cette politique et d'avoir reconnu que la protection de la vie privée des citoyens est essentielle au succès de tous ses programmes et services, y compris de l'initiative de Gouvernement en direct.

Les programmes et services actuels et nouveaux qui présentent des risques possibles en matière de vie privée sont à présent assujettis à une ÉFVP, qui est en fait une étude de faisabilité du point de vue du droit à la vie privée. Elle implique des remaniements importants de programmes actuels lorsque le remaniement porte sur une collecte, une utilisation ou une communication, nouvelle ou accrue, de renseignements personnels, un nouveau couplage de données, l'impartition ou d'autres changements qui risquent de soulever de nouvelles préoccupations relatives au droit à la vie privée.

Une ÉFVP est conçue pour donner aux ministères et organismes du gouvernement fédéral un cadre uniforme pour prévoir l'incidence d'une proposition sur le droit à la vie privée, évaluer sa conformité avec les lois et les principes sur la protection des renseignements personnels et déterminer quelles mesures d'atténuation sont requises pour surmonter les répercussions néfastes. Une ÉFVP bien exécutée permet d'éviter des frais supplémentaires, la mauvaise presse, la perte de crédibilité et de confiance du public, qui pourraient découler d'une proposition qui ne tient pas compte du droit à la vie privée. Il s'agit aussi d'une façon d'accroître la sensibilisation et la compréhension au sujet des principes de protection des renseignements personnels, tant de façon interne qu'auprès des citoyens.

La tenue d'une ÉFVP constitue une responsabilité de gestion partagée. Comme l'énonce la politique du Conseil du Trésor, les ÉFVP sont des activités de collaboration qui exigent des compétences diverses, notamment celles de gestionnaires de programme, de techniciens spécialisés, de conseillers juridiques et de conseilleurs en matière de protection des renseignements personnels. Bien qu'il incombe à l'administrateur général d'une institution, d'un ministère ou d'un organisme fédéral de déterminer s'il y a lieu de procéder à une ÉFVP, plusieurs ministères ont établi des comités internes dans le but d'examiner les projets ministériels pour déterminer si une ÉFVP est requise ou non. Compte tenu de la nature multidisciplinaire de l'exercice, cela nous semble une mesure sage.

Il est tout particulièrement important de noter que la politique exige que les ministères informent le Commissariat de toute proposition de programmes et

de services, nouveaux ou modifiés, qui soulèvent des questions relatives au droit à la vie privée. Les ministères doivent aussi consulter le Commissariat lorsqu'ils préparent une ÉFVP pour s'assurer d'identifier les risques touchant au droit à la vie privée et pour s'assurer que les mesures d'atténuation prises pour traiter de ces risques sont appropriées. En examinant la documentation de concert avec les représentants des institutions, le Commissariat est donc en mesure de donner des conseils et une orientation à ces institutions et de trouver des solutions aux risques éventuels pour la protection des renseignements personnels.

Le rôle du commissaire ne consiste pas à approuver ou à rejeter les projets évalués dans le cadre de l'ÉFVP, mais plutôt à déterminer si les ministères ont bien évalué l'incidence sur le droit à la vie privée d'un projet ou d'une proposition.

Dans le but d'assumer cette nouvelle responsabilité, nous avons créé une nouvelle division au sein de la Direction des examens et des pratiques en matière de vie privée, entièrement dédiée à l'analyse et à la présentation de commentaires sur les ÉFVP qui nous sont soumises pour examen.

Au cours de la période couverte par ce rapport, le Commissariat a reçu 17 ÉFVP et 12 évaluations préliminaires des facteurs relatifs à la vie privée (ÉPFVP), et a été consulté pour plusieurs projets qui exigeraient des ÉFVP. Compte tenu de discussions avec le Secrétariat du Conseil du Trésor (SCT) et d'autres ministères et organismes du gouvernement fédéral, nous nous attendons à recevoir plus de 50 ÉFVP au cours du prochain exercice.

La plupart de ces initiatives ou projets concernent la prestation électronique de services à des personnes par le biais du réseau Internet, de sorte que les risques en matière de protection des renseignements personnels proviennent de diverses sources, dont les caractéristiques des systèmes, l'infrastructure technique et la conception du service ou du programme électronique.

Cinq des 17 ÉFVP que nous avons reçues ont été rédigées avant l'entrée en vigueur de la politique du SCT et ainsi ne se conformaient ni aux exigences

de la politique ni aux lignes directrices associées à la politique. Par conséquent, la plupart ont été retournées aux ministères ou retirées par ces derniers pour en faire la révision conformément à la politique. Jusqu'à présent, huit ÉFVP reçues ont passé toutes les étapes du processus d'examen.

Le rôle du commissaire ne consiste pas à approuver ou à rejeter les projets évalués dans le cadre de l'ÉFVP, mais plutôt à déterminer si les ministères ont bien évalué l'incidence sur le droit à la vie privée d'un projet ou d'une proposition.

Bien que la majorité des rapports reçus jusqu'à présent des ministères concernent des ÉFVP, nous avons constaté au cours de l'année une augmentation du nombre d'évaluations préliminaires des facteurs relatifs à la vie privée (ÉPFVP). Nous pensons que cela reflète une tendance de la part des ministères à adopter une approche plus prudente et progressive à l'élaboration de leurs ÉFVP, compte tenu de leur manque de connaissances à propos du processus et du manque probable de compétences internes à cet égard. Lorsque les ministères doivent respecter une date limite fixe et imminente pour la mise en œuvre, nous leur conseillons de rédiger directement leur ÉFVP pour accélérer le processus d'examen.

Jusqu'à présent, il n'y a eu aucune ÉFVP, et certainement aucune ÉPFVP, pour lesquelles le personnel du Commissariat n'a pas jugé nécessaire de s'adresser au ministère concerné pour obtenir des renseignements supplémentaires. Parmi certains des éléments fréquemment omis, mentionnons les suivants :

- un calendrier de mise en œuvre du projet ;
- un inventaire complet des éléments de données recueillis et utilisés (les renseignements peuvent être décrits mais non détaillés) ;

- une description adéquate du processus administratif ;
- un organigramme de données ou un organigramme complet ;
- une description adéquate de l'infrastructure pour la sécurité des données associée au projet.

En outre, les documents d'information manquants comprennent souvent les suivants :

- projets d'entente où sont concernés des tiers fournisseurs de services ;
- rapports d'évaluation de la menace et des risques (EMR), le cas échéant ;
- études de faisabilité de projet, le cas échéant ;
- plans de gestion du projet, liés à la conception du projet ;
- spécifications techniques relatives à la conception du système.

Nous avons également observé un certain nombre de problèmes communs en ce qui concerne l'analyse de la protection des renseignements personnels, dont les suivants :

- la confusion de la protection des renseignements personnels avec la sécurité et la confidentialité ;
- le fait de voir le processus d'ÉFVP essentiellement comme un exercice de vérification de la conformité en matière de protection des renseignements personnels ;
- l'omission d'établir un lien entre les risques déterminés et les éléments particuliers de la conception du projet ;
- des mesures d'atténuation proposées qui ne traitent pas du risque déterminé ;
- des mesures d'atténuation proposées pour des risques non encore déterminés.

Bien que ces problèmes et omissions reflètent le manque de connaissances des ministères à propos de la politique sur l'ÉFVP, il est à noter que nous commençons maintenant à voir une amélioration générale de la qualité des ÉFVP que nous recevons.

Une des leçons à tirer de notre expérience des onze derniers mois est le besoin d'une meilleure formation sur le fonctionnement de l'ÉFVP comme mécanisme de gestion des risques. Une autre concerne la nécessité pour les ministères d'informer et de faire participer le Commissariat le plus tôt possible à l'élaboration de l'ÉFVP.

Étant donné le besoin qu'ont les organisations d'une meilleure compréhension de la politique sur l'ÉFVP, nous conseillons aux représentants du gouvernement de communiquer avec le Secrétariat du Conseil du Trésor ou de consulter son site Web à l'adresse **www.tbs-sct.gc.ca**, afin d'obtenir de plus amples informations.

DEVANT LES TRIBUNAUX

Aux termes de l'article 41 de la *Loi sur la protection des renseignements personnels*, une personne est autorisée, à l'issue d'une enquête par le Commissaire, à déposer auprès de la Cour fédérale du Canada un recours en révision d'une décision d'une institution fédérale qui lui a refusé l'accès à ses renseignements personnels. Depuis l'entrée en vigueur de la *Loi sur la protection des renseignements personnels* en 1983 jusqu'au 31 mars 2003, environ 130 recours en révision ont été déposés auprès de la Cour fédérale. Huit ont été déposés au cours de l'exercice qui a pris fin le 31 mars 2003.

L'article 42 de la *Loi sur la protection des renseignements personnels* autorise le commissaire à comparaître devant la Cour fédérale. Le commissaire peut exercer lui-même un recours en révision de la décision d'une institution fédérale qui a refusé l'accès à des renseignements personnels, dans la mesure où il obtient le consentement de la personne qui a demandé les renseignements. Il peut également comparaître devant la Cour au nom de la personne qui a exercé le recours devant elle en vertu de l'article 41 ou comparaître, avec l'autorisation de la Cour, comme partie à une instance engagée en vertu de l'article 41.

Il n'y a actuellement aucun recours judiciaire en vertu de la *Loi sur la protection des renseignements personnels* auquel le commissaire participe activement.

Toutefois, il prend également part à des litiges en dehors de l'application de la *Loi sur la protection des renseignements personnels*. Voici un résumé des litiges concernant d'importantes questions relatives au droit à la vie privée auxquels le commissaire a pris part.

Mertie Anne Beatty et autre c. Statisticien en chef et autre

Numéro du greffe T-178-02 de la Cour fédérale du Canada

Cette question a été portée devant la Cour fédérale du Canada par un groupe de citoyens canadiens qui ont demandé l'accès aux relevés du recensement de 1906 pour les provinces du Manitoba, de la Saskatchewan et de l'Alberta conformément à l'article 6 du *Règlement sur la protection des renseignements personnels*.

La position du Commissariat a toujours été que la communication des renseignements recueillis lors du recensement de 1906 est interdite par les dispositions en matière de confidentialité de la *Loi sur la statistique* et qu'on devrait, par conséquent, envisager des modifications à la *Loi* comme voie de compromis.

État de la situation

La requête a été déposée en février 2002. Après avoir examiné la loi, le gouvernement fédéral a décidé que l'information pouvait, en fait, être communiquée et fit ainsi. Le projet de loi S-13 a été présenté par la suite dans le but de modifier rétroactivement les lois sur le recensement afin de permettre l'accès aux dossiers et répondre aux préoccupations en matière de protection des renseignements personnels. En conséquence de quoi, la requête a été abandonnée.

Société canadienne des postes c. Commissaire à la protection de la vie privée

Numéro du greffe T-233-02 de la Cour fédérale du Canada

Le 14 janvier 2002, l'ancien commissaire a déterminé que le service du Programme national sur les changements d'adresse (PNCA) de la Société canadienne des postes enfreignait à deux égards la *Loi sur la protection des*

renseignements personnels. Tout d'abord, la Société canadienne des postes a enfreint le paragraphe 5(2) de la *Loi* en omettant d'informer les abonnés au service du PNCA de son intention de communiquer leurs nouvelles adresses à des expéditeurs de courrier grand public et des entreprises de marketing direct à des fins commerciales. Puis, elle a enfreint l'article 8 en omettant d'obtenir le consentement des personnes en vue de la communication de leurs nouvelles adresses aux expéditeurs de courrier grand public et aux entreprises de marketing direct.

État de la situation

Le 13 février 2002, la Société canadienne des postes a introduit une requête alléguant que l'ancien commissaire avait outrepassé ses compétences dans son application des articles 5 et 8 de la *Loi sur la protection des renseignements personnels*. Toutefois, le 4 avril 2002, la Société canadienne des postes a convenu d'ajouter une case à cocher sur son formulaire, qui permet aux personnes de consentir à cette activité. La question a donc perdu sa raison d'être et la Société canadienne des postes a abandonné sa requête le 14 avril 2002.

Commissaire à la protection de la vie privée c. procureur général du Canada et autre

Numéro du greffe S57566 de la Cour suprême de la Colombie-Britannique

Le Commissariat a reçu, en juin 2001, une plainte concernant l'installation de caméras de surveillance vidéo par la Gendarmerie royale du Canada (GRC) au centre-ville de Kelowna, C.-B. À la suite d'une enquête, l'ancien commissaire a déterminé que, par l'enregistrement continu plutôt que l'enregistrement de certains incidents liés à des activités d'application de la loi, la GRC recueillait inutilement des renseignements sur des milliers de citoyens innocents se livrant à des activités qui n'avaient nullement rapport avec le mandat de la GRC. Par conséquent, il a conclu que la surveillance vidéo à Kelowna enfreignait la *Loi sur la protection des renseignements personnels*.

La GRC a informé le Commissariat qu'elle avait mis fin, le 28 août 2001, à l'enregistrement vidéo continu par caméra de surveillance vidéo. Ce faisant, il n'y aurait enregistrement vidéo du secteur sous surveillance que si une infraction à la loi était constatée. Bien que cela assure la conformité de l'utilisation de la caméra de surveillance vidéo avec la lettre de la *Loi sur la protection des renseignements personnels*, qui ne s'applique techniquement qu'aux renseignements « quels que soient leur forme et leur support », l'ancien commissaire était d'avis que la poursuite de la surveillance par caméra vidéo même en l'absence d'enregistrement continu ne respecte pas suffisamment l'esprit de la *Loi sur la protection des renseignements personnels* et de la protection des droits à la vie privée des Canadiens et Canadiennes.

Le 21 juin 2002, l'ancien commissaire a déposé une déclaration à la Cour suprême de la Colombie-Britannique, pour demander que la Cour déclare que cette surveillance vidéo généralisée était inconstitutionnelle, enfreint la *Charte*, ainsi que les obligations internationales du Canada en matière de droits de la personne. Du 12 au 14 mars 2003, une audience a été tenue concernant la requête du gouvernement fédéral demandant à la cour de rejeter la cause. La cour a statué que le commissaire n'était pas légalement habilité à intenter une action en justice.

État de la situation

Le 4 juillet 2003, le commissaire nouvellement nommé a annoncé que le Commissariat avait demandé à l'avocat de retirer son appel relatif à l'affaire. Bien que le commissaire et le Commissariat aient toujours diverses préoccupations en ce qui a trait à la surveillance vidéo des endroits publics par des autorités publiques, le fait de poursuivre cette action particulière n'était pas perçu comme un moyen efficace de dépenser les fonds publics.

Commissaire à l'information du Canada c. Commissaire de la GRC et autre

Numéro du greffe 28601 de la Cour suprême du Canada

Une liste des affectations de quatre agents de la Gendarmerie royale du Canada (GRC) avait fait l'objet d'une demande aux termes de la *Loi sur l'accès à l'information*. Le commissaire de la GRC a refusé de communiquer les renseignements parce qu'ils se rapportaient aux antécédents professionnels de ces personnes et qu'il s'agissait ainsi de renseignements personnels aux termes de l'article 3 de la *Loi sur la protection des renseignements personnels*. Le commissaire à l'information a soutenu toutefois que l'alinéa 3 *j*) portant sur la définition de renseignements personnels dans la *Loi sur la protection des renseignements personnels* stipule que les renseignements relatifs aux postes ou fonctions d'agents ou de fonctionnaires du gouvernement ne constituent pas des renseignements personnels pour l'application de l'article 19 de la *Loi sur l'accès à l'information*.

État de la situation

Le 6 mars 2003, la Cour suprême du Canada a fait part de sa décision unanime. La Cour a très clairement déclaré que l'information peut être personnelle et néanmoins être visée par la rubrique de l'alinéa 3 *j)* qui précise les caractéristiques générales associées au poste ou fonctions d'un agent ou d'un fonctionnaire d'une institution fédérale. La Cour suprême a estimé qu'aucun des renseignements demandés ne concernait la compétence ou les caractéristiques des employés. Par conséquent, elle a ordonné que les renseignements suivants soient communiqués pour chacune des personnes nommées : une liste des affectations antérieures, avec statut et dates, une liste des grades et les dates auxquelles ces grades ont été obtenus, ainsi que les années de service et la date d'anniversaire du service.

La décision de la Cour suprême restreint l'application de l'alinéa 3 *j)* relatif à la définition de renseignements personnels. Bien que le Commissariat ait plaidé en faveur d'une interprétation plus restreinte de l'exception, la décision de la Cour suprême n'est pas sans fondement.

Partie II

Rapport concernant la *Loi sur la protection des renseignements personnels et les documents électroniques*

INTRODUCTION

La *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ)* établit des règles de base sur la façon dont les organisations du secteur privé peuvent recueillir, utiliser et communiquer des renseignements personnels dans le cadre de leurs activités commerciales.

Depuis l'entrée en vigueur de la *Loi*, le 1er janvier 2001, elle s'est principalement appliquée aux activités commerciales de ce qu'on appelle les installations, les ouvrages, les entreprises ou les secteurs d'activité fédéraux, notamment les entreprises de transport et de télécommunications, les banques et les radiodiffuseurs. Elle s'applique aussi aux renseignements personnels des employés de ces entreprises, ainsi qu'à la vente, à la location ou au troc de renseignements personnels au-delà des frontières provinciales ou nationales par des organisations sous réglementation provinciale. Depuis le 1er janvier 2002, les renseignements personnels sur la santé recueillis, utilisés ou communiqués par ces organisations sont aussi couverts. À compter du 1er janvier 2004, la *LPRPDÉ* portera également sur la collecte, l'utilisation ou la communication de renseignements personnels dans le cadre de toutes les activités commerciales au Canada, sauf dans les provinces qui auront adopté une loi jugée essentiellement similaire à la loi fédérale.

La deuxième année complète d'application de la *LPRPDÉ* s'est avérée à la fois intéressante et stimulante pour le Commissariat à plusieurs égards. Nous avons commencé à recevoir des plaintes concernant les renseignements personnels sur la santé des personnes et à faire enquête sur ces plaintes. Nous avons aussi fait des percées importantes sur une kyrielle de questions, dont le consentement et le marketing, la cote de solvabilité, l'enregistrement des appels téléphoniques et les autorisations de sécurité.

Nous avons aussi entrepris un certain nombre d'activités de communication en vue d'une sensibilisation sur les questions liées au droit à la vie privée et sur les lois fédérales concernant la protection des renseignements personnels. Du 1er avril 2002 au 31 mars 2003, l'ancien commissaire et les cadres supérieurs ont prononcé 49 allocutions lors de conférences et événements spéciaux ; nous avons émis plus de 25 communiqués et avis aux médias sur des questions-clé touchant au droit à la vie privée ; nous avons répondu à des centaines de demandes de renseignements et d'entrevues adressées par les médias ; nous avons distribué plus de 23 000 exemplaires de nos publications à des particuliers, à des entreprises et autres organisations à travers le pays ; et nous avons reçu un nombre plus croissant que jamais de visites sur notre site web, soit en moyenne 50 000 visites par mois.

En vertu de la *LPRPDÉ*, le commissaire est tenu de soumettre un rapport annuel au Parlement sur les activités du Commissariat au cours de l'exercice antérieur. En ce qui concerne la *LPRPDÉ*, le présent rapport porte sur la période du 1er janvier 2002 au 31 décembre 2002.

ENQUÊTES ET DEMANDES DE RENSEIGNEMENTS

Au cours de l'année civile 2002, le Commissariat a reçu 300 plaintes en vertu de la *LPRPDÉ* de personnes alléguant que leurs droits à la vie privée avaient été enfreints par toute une gamme d'organisations. Environ 37 % des cas portaient sur des pratiques du secteur bancaire, suivis de 19 % dans les secteurs des télécommunications et la radiodiffusion, 15 % dans les entreprises de transport et 13 % dans le secteur nucléaire. Le reste des

plaintes, 16 %, avait été déposé à l'endroit d'autres types d'organisations, dont les fournisseurs d'accès Internet, les agences d'évaluation du crédit et les conseils de bandes autochtones.

En 2002, l'ancien commissaire a rendu des conclusions sur 162 plaintes déposées en vertu de la *LPRPDÉ*, comme suit :

Non fondées	61
Fondées	45
Résolues	41
Abandonnées	15

De plus, le Commissariat a aussi mené cinq enquêtes sur des incidents. Les incidents sont des questions provenant de diverses sources, notamment les médias, dont le commissaire prend connaissance. Habituellement dans pareil cas, la victime n'est pas nommée et le Commissariat n'a reçu aucune plainte.

Ce qui suit dans ce rapport constitue des exemples des cas les plus notables de l'année. Des résumés plus détaillés de toutes les conclusions en vertu de la *LPRPDÉ* se trouvent sur notre site Web à l'adresse **www.privcom.gc.ca**. Ces conclusions sont affichées dans le but de donner une orientation aux organisations et à la collectivité juridique sur l'application de la *Loi*.

DÉFINITION DE CONCLUSIONS EN VERTU DE LA *LPRPDÉ*

Non fondée : Cela signifie qu'il n'y a pas de preuve qui porte le commissaire à la protection de la vie privée à conclure que l'organisation a enfreint la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ)*.

Fondée : Cela signifie que l'enquête a révélé que l'organisation n'a pas respecté une des dispositions de la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ)*.

Résolue : Cela signifie que l'organisation a pris des mesures correctives pour remédier à la situation, ou que le plaignant est satisfait des résultats de l'enquête menée par le Commissariat à la protection de la vie privée du Canada.

Abandonnée : Il s'agit d'une enquête qui a pris fin avant que toutes les allégations n'aient été pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons, par exemple, lorsque le plaignant n'est plus intéressé à donner suite à l'affaire.

SOMMAIRE DE CAS CHOISIS EN VERTU DE LA *LPRPDÉ*

Cas portant sur une erreur sur la personne

Une plaignante a écrit au Commissariat pour signaler qu'un ami l'avait informé d'un avis paru dans le journal selon lequel elle était recherchée par la police. À sa grande horreur, la plaignante a vu sa propre image dans une photographie accompagnant l'article « Crime de la semaine » d'*Échec au crime*. L'article faisait état d'un récent vol de deux chèques d'une femme âgée et désignait la personne illustrée comme suspecte du crime. L'image avait été saisie par une caméra de surveillance vidéo à la banque. La caméra était braquée sur le guichet de la caissière où le voleur avait encaissé les chèques volés.

Il s'est avéré que la plaignante s'était en effet présentée à la même banque et au même guichet le jour en question, mais non pas pour encaisser un chèque. Elle y était allée simplement pour régler une facture. Il était clair qu'elle n'était pas l'auteur du crime.

Comme notre enquêteur l'a appris, il s'agissait de la même banque, du même guichet, du même jour, mais non de la même heure.

Le jour en question, l'horloge de la bande journal de la banque (son registre central informatisé de toutes les transactions) avait 12 minutes de retard sur l'horloge de la caméra vidéo. Lorsque le personnel de sécurité a fait avancer la

bande vidéo jusqu'à l'heure de l'encaissement indiquée par la bande journal, l'image qui apparaissait n'était pas celle de la vraie personne qui avait encaissé les chèques. C'était plutôt celle de la femme qui avait précédé la personne qui avait encaissé les chèques au guichet de la caissière quelque 12 minutes plus tôt, c'est-à-dire la plaignante.

*À sa grande horreur, la plaignante a vu sa propre image dans une photographie accompagnant l'article « Crime de la semaine » d'*Échec au crime.

Ainsi, les photos que la banque a remises par la suite au service de police local, et que la police a à son tour donné à l'organisme *Échec au crime*, illustraient la mauvaise personne.

Une semaine après l'article « Crime de la semaine » initial, *Échec au crime* a corrigé l'erreur en publiant une rétractation dans le même quotidien. Le même jour, le journal a publié, en page de couverture, un article précisant que la plaignante avait été la victime d'une erreur sur la personne. La plaignante a reçu des excuses officielles de la banque, de la police et d'*Échec au crime*. La police et *Échec au crime* ont tous deux admis par la suite ne pas avoir suivi les procédures normales de vérification dans ce cas et tous deux ont depuis collaboré à l'élaboration de mesures visant à prévenir des situations semblables. La banque a aussi mis en œuvre des changements de procédure pour vérifier les heures des bandes vidéo de surveillance et des bandes journal.

Toutefois, la plaignante n'était pas entièrement satisfaite. Après le choc initial et le bouleversement, elle est devenue bien plus préoccupée par l'effet qu'avait l'incident sur sa réputation, lorsqu'elle a appris que de nombreuses personnes l'avaient bel et bien reconnue dans l'article. Cela était tout particulièrement inquiétant, parce que son travail dépendait de sa capacité de se rendre aux résidences et aux lieux de travail de ses clients. Elle était aussi préoccupée du

fait que son image avait peut-être paru dans d'autres avis d'*Échec au crime*. Le Commissariat a pu rassurer la plaignante que sa photographie n'avait paru que dans un seul article de journal.

En ce qui concerne la résolution de sa plainte officielle adressée à l'ancien commissaire, nous avons examiné la question en fonction des obligations qu'a la banque, en vertu de la *LPRPDÉ*, d'assurer l'exactitude des renseignements personnels.

Nous avons déterminé que les renseignements personnels en question – la photographie de la plaignante – étaient entièrement inexacts dans une situation où l'exactitude avait été décisive dans le but de résoudre un crime. Pour cette raison seulement, la banque aurait dû s'assurer que l'information communiquée était aussi exacte que possible. Elle ne l'a pas fait et, par conséquent, elle a clairement enfreint le principe 4.6 de la *Loi*. Dans sa lettre de conclusion adressée à la plaignante, l'ancien commissaire a écrit :

> *« ...une organisation doit bien tenir compte des conséquences néfastes possibles de renseignements inexacts sur une personne. J'ai déterminé que vos renseignements personnels communiqués de façon inappropriée par [la banque] ont servi à prendre une décision à votre sujet – en particulier, une décision erronée selon laquelle vous étiez recherchée en tant que suspecte principale d'un crime. Qui plus est, ce fut une décision qui vous a causé une triste réputation, de l'embarras et des inquiétudes à propos de votre réputation et de votre gagne-pain. Sachant bien que la police se servirait probablement de vos renseignements personnels pour vous soupçonner d'un crime, [la banque] aurait dû prendre soin de veiller à l'exactitude de ces renseignements afin de réduire la possibilité d'une mauvaise décision aux conséquences défavorables pour vous.* » [traduction]

L'ancien commissaire a déterminé que cette plainte était fondée.

Des pilotes canadiens affectés par des mesures de sécurité prises par les États-Unis

Les Canadiennes et Canadiens moyens continuent de ressentir les contrecoups des événements du 11 septembre 2001. Une personne directement touchée par les nouvelles mesures de sécurité, un pilote d'une compagnie aérienne commerciale, s'est vu confronté à un choix difficile : renoncer à ses droits à la vie privée ou risquer de perdre son emploi. Dans le passé, lorsque le pilote devait suivre une formation de pilotage requise pour maintenir son permis, son employeur l'inscrivait simplement à une école de pilotage en Floride. Cette procédure a changé après le 11 septembre 2001. Les écoles de pilotage américaines sont à présent tenues de faire signer un formulaire d'autorisation par leurs étudiants étrangers, y compris les pilotes canadiens de compagnies aériennes commerciales. Ce formulaire permettrait au gouvernement des États-Unis de recueillir et de communiquer des renseignements personnels concernant les étudiants. Toutefois, il n'a pas adéquatement expliqué les raisons de cette collecte et communication, ni n'a semblé établir des limites à cet égard.

Lorsque son employeur lui a demandé de signer le formulaire, le pilote était outré. Après tout, le gouvernement canadien avait déjà fait une vérification approfondie de ses antécédents. Il n'aimait pas l'idée d'un gouvernement étranger passant au crible ses antécédents, d'autant plus qu'il ne savait pas clairement quels renseignements seraient recueillis et à qui ils seraient communiqués.

Il n'aimait pas l'idée d'un gouvernement étranger passant au crible ses antécédents, d'autant plus qu'il ne savait pas clairement quels renseignements seraient recueillis et à qui ils seraient communiqués.

Personne ne semblait à l'aise relativement au formulaire – le

gouvernement canadien, la compagnie de transport aérien, le syndicat – mais il n'y avait aucune solution immédiate à l'horizon. Le gouvernement fédéral avait demandé aux États-Unis d'accepter la vérification, faite au Canada, des antécédents des pilotes de compagnies aériennes commerciales. Mais, au moment de la plainte, les États-Unis n'avaient pas encore pris de décision.

La compagnie de transport aérien était troublée par le libellé du formulaire, mais se trouvait dans une situation difficile. La loi exige que ses pilotes soient formés. L'autre école de pilotage la plus proche se trouvait en Europe – ce qui aurait été plus coûteux que d'envoyer ses pilotes en Floride. De plus, étant donné que le pilote et le copilote doivent recevoir la formation en même temps, la compagnie de transport aérien se trouverait dans une position délicate si un pilote était disposé à signer le formulaire tandis que l'autre ne l'était pas.

Le syndicat des pilotes a protesté contre l'exigence de signer le formulaire. Il a négocié une entente avec la compagnie de transport aérien qui stipule, entre autres, que la décision de signer le formulaire était volontaire et que la compagnie offrirait une formation de rechange aux pilotes qui s'y opposaient.

Le pilote a décidé de ne pas signer le formulaire. Bien que son employeur ait obtenu une prorogation temporaire de son permis jusqu'à ce qu'une solution puisse être trouvée, il n'a pris aucune autre disposition en vue d'une formation pour lui. À moins que le gouvernement américain n'accepte la demande du Canada ou que l'ancien commissaire à la protection de la vie privée ne rende ses conclusions, la compagnie de transport aérien refuserait de modifier sa décision. La prorogation du permis du pilote est finalement venue à échéance.

Nous nous sommes vivement opposés au formulaire d'autorisation. Nous l'avons trouvé tout à fait inadmissible à de nombreux égards et nous avons conclu que les pratiques qu'il autorisait ne respectaient pas du tout les principes équitables en matière de traitement de l'information, qui sont la pierre angulaire des lois sur la protection des renseignements personnels au Canada.

Pour parvenir à cette décision, nous nous sommes fiés au « critère de la personne raisonnable » énoncé au paragraphe 5(3) de la *LPRPDÉ* afin d'évaluer les buts de la compagnie de transport aérien. Nous avons reconnu que les motifs de la compagnie exigeant que ses pilotes signent un tel formulaire semblaient raisonnables à première vue. Toutefois, au-delà des apparences, les motifs cessent d'être acceptables. Nous avons estimé qu'il n'était pas vraiment à l'honneur de la compagnie de transport aérien de faire passer le coût et la commodité avant le droit du pilote de refuser de consentir à des pratiques de collecte et de communication qui contrevenaient manifestement à la loi canadienne. Nous avons fait remarquer que la compagnie de transport aérien avait des options, mais avait choisi de ne pas s'en prévaloir.

En déterminant que les motifs de la compagnie de transport aérien ne se conformaient pas aux exigences du paragraphe 5(3), l'ancien commissaire a émis, dans sa lettre de conclusion, le commentaire suivant sur cet exemple opportun concernant la difficulté à tenir l'équilibre entre les exigences en matière de sécurité et le droit fondamental à la vie privée :

> *« Je conviens que les circonstances dans lesquelles se trouvent de nombreux pays, tout particulièrement les États-Unis, justifient la prise de certaines mesures de sécurité. Naturellement, il est raisonnable d'exiger que les pilotes reçoivent une autorisation de sécurité afin de pouvoir voler et c'est la raison pour laquelle le Canada a établi des mesures de sécurité auxquelles sont assujettis les pilotes de compagnies aériennes commerciales au Canada... Mais est-ce qu'une personne raisonnable trouverait qu'il est approprié d'exiger que ces mêmes pilotes consentent à des pratiques inacceptables de collecte et de communication de renseignements personnels à la demande d'un gouvernement étranger? Je ne le crois pas. En fait, je soupçonne que la plupart des Canadiens et Canadiennes raisonnables trouveraient que cet empiètement sur les droits canadiens est hautement inadmissible et exigeraient que l'employeur offre des options raisonnables aux employés et que le gouvernement soulève la question avec les États-Unis.* » [traduction]

Après avoir reçu la lettre de conclusion, la compagnie de transport aérien a accepté la recommandation de l'ancien commissaire et pris des dispositions pour offrir la formation à un autre endroit au pilote et aux autres personnes qui refusaient de signer le formulaire.

Communication inappropriée, par une banque, de renseignements personnels à l'employeur de l'intéressé

Une personne s'est présentée à sa banque pour une affaire personnelle : contester les frais pour des chèques. Il n'était pas satisfait de la réponse de la banque et une dispute a eu lieu.

Le directeur de la succursale est entré en scène et a décidé que son personnel n'avait plus à composer avec le client. Il s'est trouvé que l'entreprise qui employait le client faisait d'importantes affaires avec la banque. Avant de mettre fin à la relation entre la banque et le client, le directeur de la succursale a jugé bon de discuter de cette question avec l'employeur du client.

Le plaignant était surpris lorsque son employeur l'a confronté au sujet de ce qui s'était passé plus tôt ce matin-là à la banque.

L'une de nos premières tâches dans cette enquête était de déterminer exactement ce qui avait été communiqué par téléphone entre le directeur de la banque et l'employeur. Puisque rien ne prouvait qu'ils avaient discuté des affaires financières du plaignant, il semblait que la communication effective avait été limitée à trois simples faits : (1) que le plaignant avait un compte à cette succursale ; (2) que son compte serait bientôt fermé ; (3) qu'il y avait eu une scène avec le caissier ou la caissière.

Selon la banque, rien de cela ne peut être considéré comme étant des renseignements personnels concernant le plaignant. La banque a souligné que la scène, elle-même, s'était produite dans un endroit public et dans une petite communauté, à un endroit où le fait d'effectuer des opérations bancaires est difficilement affaire de secret. La position prise par la banque était que la communication en question entrait dans la catégorie du « discours

public normal », comparable à des « potins anodins ». La banque a même suggéré qu'elle avait le droit de communiquer de tels renseignements dans un souci de « courtoisie commerciale » et de protection de ses propres intérêts. En citant le paragraphe 5(3) et le principe 4.3.5, les soi-disantes dispositions relatives à la « raisonnabilité » de la *LPRPDÉ*, la banque a également suggéré que le plaignant n'avait aucune attente raisonnable en matière de protection de la vie privée et que des personnes raisonnables auraient considéré la communication appropriée dans les circonstances.

Bien que nous n'ayons pas été rébarbatifs face à la banque et que nous ayons été prêts à concéder jusqu'à un certain point le caractère raisonnable du point de vue de la banque, l'ancien commissaire devait établir la distinction quelque part. En présentant ses conclusions au plaignant, il a formulé le commentaire suivant :

> *« À mon avis,... le caractère raisonnable de la situation s'arrête exactement au point où le directeur [de la banque], sachant que vous aviez agi en votre propre nom à sa succursale ce matin-là, a néanmoins pris le téléphone à son bureau pendant les heures de travail pour informer votre employeur. Ce n'était pas une communication anodine ou par inadvertance. Ce n'était pas des potins anodins. Il s'agissait d'un acte délibéré de communication de renseignements personnels à un tiers par une personne agissant en sa qualité officielle, qui n'était nullement habilité à faire cette communication. En outre, la* Loi *place les droits des personnes au-dessus de notions comme la « courtoisie commerciale » et ne fait pas de distinction quant à la taille de la localité qu'habite la personne. Y a-t-il quelque part une personne raisonnable qui s'attendrait à ce que son directeur de banque communique à son employeur des renseignements concernant ses affaires bancaires personnelles? La réponse à cette question est évidemment non. »* [traduction]

Une fraude relative à la cote de crédit

Au cours d'enquêtes sur les plaintes concernant l'évaluation de solvabilité et l'attribution de cotes de crédit, nous avons beaucoup appris sur le fonctionnement de l'industrie d'octroi de crédit en général.

Dans deux cas particuliers, les personnes avaient fait des demandes officielles en vertu de la *LPRPDÉ* afin d'avoir accès à certains renseignements personnels contenus dans des dossiers détenus par leurs banques. Plus particulièrement, chaque requérant voulait connaître sa cote de crédit. Les banques en question leur en ont refusé l'accès, invoquant la disposition d'exemption stipulée au paragraphe 9(3)*b*) de la *Loi*. Cette disposition stipule, de fait, qu'une organisation n'est pas tenue de communiquer à l'intéressé des renseignements personnels, dans le cas où la communication « révélerait des renseignements commerciaux confidentiels ».

Au cours d'enquêtes sur les plaintes concernant l'évaluation de solvabilité et l'attribution de cotes de crédit, nous avons beaucoup appris sur le fonctionnement de l'industrie d'octroi de crédit en général.

Les requérants, croyant au contraire que les cotes de crédit constituaient des renseignements personnels auxquels ils avaient pleinement le droit d'avoir accès, ont porté plainte au Commissariat. Notre tâche principale, dans chacun des cas, consistait à déterminer si l'exemption citée par la banque était valide.

Une cote de crédit correspond à une indication numérique de la capacité financière, calculée grâce à un modèle algorithmique. Pour la plupart des gens qui connaissent bien cette notion, le terme « cote de crédit » évoque généralement les agences d'évaluation de solvabilité. Ces agences offrent aux banques et aux autres institutions d'octroi de crédit des services de renseignements sur les antécédents en matière de solvabilité de clients potentiels, y compris parfois les cotes de crédit. En examinant une demande de crédit, une institution d'octroi de crédit obtiendra souvent les antécédents en matière de solvabilité du demandeur par une agence d'évaluation de

solvabilité. Dans certains cas, l'institution demandera également une cote de crédit pour le demandeur. Les agences d'évaluation de solvabilité ne calculent pas elles-mêmes les cotes de crédit, mais fournissent plutôt des cotes calculées par une autre entreprise à partir des renseignements détenus par l'agence.

Jusqu'à un certain point, les plaignants avaient de bonnes raisons pour maintenir une telle position. Dans des cas antérieurs, nous avions déjà examiné la question d'accès aux renseignements personnels sur la solvabilité, du moins dans les où des agences d'évaluation de solvabilité étaient impliquées. Nous avions déjà conclu que les cotes de crédit constituent des renseignements personnels selon la définition de la *Loi* et que les personnes ont le droit, en principe, d'y avoir accès. Nous avons déterminé que les agences d'évaluation de solvabilité en particulier doivent se conformer au principe 4.9 de la *Loi* en donnant aux personnes, lorsqu'elles le demandent, accès aux renseignements personnels les concernant contenus dans leur dossier de solvabilité. De plus, nous avons déterminé que les banques, si elles ont obtenues les antécédents de solvabilité d'une personne par une agence d'évaluation de crédit, devaient, dans le même ordre d'idées, donner à la personne accès aux renseignements lorsque celle-ci en fait la demande, y compris la cote de crédit calculée par l'agence.

Mais les cas les plus récents n'étaient pas aussi explicites. Le problème particulier qu'ils ont soulevé était que les cotes de crédit demandées par les plaignants n'étaient pas les cotes de crédit habituelles fournies par les agences d'évaluation de solvabilité. Il s'agissait, en réalité, de cotes de crédit que les banques elles-mêmes avaient calculées et attribuées au niveau interne.

Le fait que les banques aussi possèdent leurs propres cotes de crédit, distinctes de celles fournies par les agences d'évaluation de solvabilité, est généralement moins connu. Les banques calculent leurs propres cotes de crédit internes grâce à leurs propres modèles d'attribution de cote de crédit internes, très différents de ceux qui sont associés aux agences. Tandis que les cotes des agences sont calculées au moyen de modèles standardisés basés presque exclusivement sur les renseignements de solvabilité, une banque élabore des modèles personnalisés tout particuliers, propres à elle et incorporant non

seulement les renseignements de solvabilité sur la personne mais également plusieurs autres éléments relatifs aux priorités stratégiques commerciales de la banque. Étant donné que les banques considèrent et traitent leurs modèles internes d'attribution de cotes de crédit comme des renseignements commerciaux confidentiels faisant l'objet d'une propriété exclusive, de tels modèles sont plus problématiques du point de vue de la *Loi*.

Le problème particulier qu'ils ont soulevé était que les cotes de crédit demandées par les plaignants n'étaient pas les cotes de crédit habituelles fournies par les agences d'évaluation de solvabilité.

En invoquant le paragraphe 9(3)*b*), les banques en question ne suggéraient pas qu'une cote de crédit calculée au niveau interne constituait en elle-même des renseignements commerciaux confidentiels, mais plutôt que le modèle utilisé pour calculer une telle cote constituait des renseignements commerciaux confidentiels. Par conséquent, disaient-elles en fait, si les cotes de crédit internes étaient rendues disponibles aux personnes, cela aurait pour effet de faire connaître le modèle avec lequel les cotes sont calculées.

Nous avons accepté les arguments des banques selon lesquels le modèle interne d'évaluation de solvabilité représentait un renseignement commercial confidentiel. Mais nous étions beaucoup moins persuadé par l'affirmation plus décisive selon laquelle le fait de communiquer les cotes de crédit pourrait révéler de quelque façon le modèle d'attribution de la côte de crédit lui-même. Comment le simple fait de communiquer à une personne sa cote de crédit pourrait vraisemblablement l'amener à connaître le fonctionnement restreint d'une telle approche logarithmique, technique et compliquée comme le modèle d'attribution d'une cote de crédit?

En réalité, les banques ne craignaient pas le client moyen, mais les fraudeurs qui essaient de « décoder » le modèle interne d'attribution de cote de crédit à des fins néfastes. Selon les banques, les fraudeurs pourraient employer des moyens détournés pour obtenir un certain nombre de cotes de crédit et pourraient extrapoler le modèle à partir de ces cotes. Les fraudeurs peuvent soit travailler pour des fournisseurs de crédit concurrents des banques, qui essaient de bénéficier d'avantages concurrentiels, soit travailler à leur propre compte, essayant d'obtenir du crédit pour eux-mêmes sur de fausses déclarations.

Dans leurs observations, les banques ont présenté au Commissariat une analyse judiciaire des risques de fraude liés à la disponibilité des cotes de crédit. Cette analyse a conclu que si les cotes de crédit étaient immédiatement accessible, l'intégrité du modèle d'attribution des cotes de crédit d'une banque pourrait être compromise à partir d'un nombre relativement restreint de cotes de crédit calculées grâce au modèle.

Les scénarios de fraude soulignés par les banques nous ont semblé étranges. Cependant, afin d'être équitables, nous avons demandé conseil à un spécialiste dans le domaine des algorithmes. Ce spécialiste a confirmé qu'avec l'accès aux cotes de crédit personnalisées, il serait assurément plus facile de reproduire approximativement le modèle d'attribution de cotes de crédit interne d'une banque.

Nous en doutions encore. Plus particulièrement, nous étions conscients que l'alinéa 9(3)*b*), qui utilise le mot « révélerait » plutôt que « pourrait révéler », place la barre très haute pour qui voudrait justifier le refus de communiquer des renseignements personnels. En ce qui concerne l'avis du spécialiste en algorithmes, nous étions disposés à admettre qu'il serait techniquement possible de reproduire approximativement un modèle à partir d'un certain nombre de cotes, mais nous n'étions pas persuadés que cela pourrait se produire. Les observations présentées par les banques ne nous ont pas convaincus que des fraudeurs iraient vraiment jusqu'à agir de la façon décrite dans l'analyse du risque dans le seul but de tromper une banque. Nous étions particulièrement sceptiques à l'égard de la crainte, de toute évidence partagée

par toutes les banques, selon laquelle les fournisseurs de crédit concurrents auraient recours, en fait, à de telles tactiques pour « déchiffrer » les modèles des uns des autres dans le souci de bénéficier d'un avantage concurrentiel.

Cependant, il reste que deux banques avaient fermement exprimé ce qui nous est apparu comme une profonde conviction et une crainte selon lesquelles des modèles d'attribution de cotes de crédit seraient inévitablement révélés et manipulés de manière frauduleuse, si des personnes avaient accès aux cotes de crédit. Quoique cela nous ait semblé improbable, il était indéniable que les banques s'inquiétaient sérieusement de cette possibilité, que nous avons, par ailleurs, été incapables de réfuter.

En fin de compte, l'ancien commissaire a décidé d'accorder le bénéfice du doute aux banques. Il l'a fait principalement en raison de son devoir d'équilibrer les droits à la vie privée des personnes et les intérêts légitimes des organisations en matière de renseignements. Considérant la faible valeur informative de la cote de crédit en tant que telle et le fait que l'impossibilité d'obtenir des cotes de crédit internes ne portait pas atteinte de façon significative aux droits à la vie privée des Canadiens et des Canadiennes, nous avons jugé qu'il était tout à fait juste, dans de telles circonstances, d'accepter la position des banques.

L'ancien commissaire a conclu que les banques avaient invoqué de façon appropriée l'alinéa 9 (3)*b*) pour refuser aux plaignants l'accès à leurs cotes de crédit internes.

Clients, faites attention! Vos conversations pourraient être enregistrées

La pratique d'enregistrement des appels téléphoniques des clients – pratiques assez répandues dans plusieurs organisations – a fait l'objet de deux plaintes. Ces cas illustrent deux approches très différentes prises par les organisations pour informer leurs clients de cette pratique et pour obtenir leur consentement. Dans les deux cas, ainsi que dans ceux impliquant le marketing à des fins secondaires, les attentes raisonnables ont joué un rôle important dans les conclusions de l'ancien commissaire.

... la plupart des gens souhaiteraient être informé avant que leur appel va ou pourrait être enregistré.

Dans le premier cas, une personne a téléphoné à sa banque dans le but de se porter garant dans la demande de prêt de sa fille. À la fin de la conversation, il a appris que l'appel avait été enregistré. Il n'avait pas été informé, ni par le représentant du service à la clientèle ni par l'entremise d'un message enregistré, que son appel serait enregistré. On ne lui a pas non plus demandé, après qu'il a appris que son appel avait été enregistré, s'il était d'accord.

La banque avait un point de vue intéressant sur la question du consentement dans de cas. Selon elle, une seule des parties avait à consentir à l'enregistrement des appels. La banque exigeait donc de ses agents de service à la clientèle qu'ils signent un document confirmant leur consentement à l'enregistrement de ces appels.

L'objectif de la banque concernant l'enregistrement des appels était lié au fait qu'elle avait besoin d'une confirmation de la demande du client, ainsi qu'une preuve de son consentent aux modalités du produit ou du service. Selon la banque, l'appel enregistré équivaut à un formulaire signé et est utilisé pour la tenue de dossiers.

Nous sommes d'accord sur le fait que l'information échangée au cours de la conversation devrait être enregistrée d'une certaine façon. Cependant, les attentes raisonnables du client devraient également être prises en considération et la plupart des gens souhaiteraient être informées *avant* que leur appel soit ou puisse être enregistré. Dans ce cas, la banque ne répondait pas du tout à ces attentes et n'avait pas obtenu le consentement du père pour enregistrer cet appel, contrevenant ainsi au principe de consentement de la *LPRPDÉ*.

Dans le cas de l'autre plainte, une personne allègue que sa banque avait enregistré ses conversations téléphoniques à son insu et sans son

consentement. Cette personne avait engagé des procédures judiciaires en cour contre la banque, qu'il tenait responsable de certains retraits effectués avec sa carte bancaire. Au cours de ce processus, la banque a déposé en preuve l'enregistrement d'une conversation téléphonique entre lui et un employé de la banque.

La banque a soutenu qu'elle avait obtenu le consentement de la personne pour enregistrer ses appels. Elle a fait référence à une entente signée par le plaignant lorsqu'il a ouvert son compte, laquelle reconnaissait la pratique d'enregistrement des appels téléphoniques par la banque. Le plaignant avait aussi reçu des brochures sur la protection des renseignements personnels (cinq en tout), qui expliquaient les fins pour lesquelles la banque recueillait des renseignements personnels. Cependant, le plaignant n'avait lu aucun des documents qui lui avaient été remis.

Puis, il y avait la conversation entre un employé de la banque et le plaignant (également enregistrée), dans laquelle l'employé expliquait la pratique d'enregistrement des conversations de la banque. Selon le plaignant, le terme « enregistrement » ne signifiait pas nécessairement enregistrement électronique et il a maintenu sa plainte originale.

L'ancien commissaire a déterminé que la banque avait fait un effort raisonnable pour informer le plaignant de sa pratique, ainsi que de l'objectif de cette pratique, et qu'elle avait obtenu son consentement pour enregistrer ses appels en raison de l'entente qu'il avait signée. Par conséquent, nous avons conclu que la banque s'était conformée aux dispositions pertinentes de la *Loi*.

Il est clair que des organisations comme celle-ci, qui ont fait un effort pour informer leurs clients et obtenir leur consentement, ont une attente raisonnable à l'égard du fait que les clients liront les documents qui ont été portés à leur attention.

Néanmoins, la banque dans le deuxième cas était prête à améliorer davantage ses pratiques concernant l'enregistrement des appels téléphoniques. En réponse à cela, le Commissariat a élaboré des lignes directrices sur les « pratiques exemplaires » pour l'enregistrement des appels téléphoniques des clients. En substance, ces lignes directrices soulignent le fait que l'enregistrement des appels téléphoniques implique la collecte de renseignements personnels – une pratique qui devrait respecter les principes équitables de traitement de l'information. En d'autres termes, les conversations ne doivent pas être enregistrées à moins que l'enregistrement ne serve à des fins que toute personne raisonnable considérerait appropriées dans les circonstances. Le client doit être informé de la fin pour laquelle l'appel est enregistré et y consentir, sauf dans un nombre restreint de cas où le consentement n'est pas exigé, et ce avant que l'enregistrement ne commence. Le client devrait également avoir des solutions de rechange telles que celles qui consistent à ne pas enregistrer l'appel, à visiter un point de vente au détail, à rédiger une lettre ou à effectuer une transaction sur Internet.

Un enregistrement sur bande magnétique saisit plus que les données précises nécessaires au but de l'appel. Il enregistre les commentaires, les accents, les attitudes – des renseignements qui peuvent ne pas être pertinents à la documentation nécessaire. C'est pour ces raisons qu'il est important pour les organisations d'être ouvertes avec les clients, de les informer que leur conversation sera enregistrée, d'expliquer pourquoi elle sera enregistrée et de leur offrir des options s'ils ne souhaitent pas être enregistrés.

Dan les deux cas, nous avons fourni aux banques nos lignes directrices sur les « pratiques exemplaires » et les deux organisations ont entrepris d'apporter des améliorations à leurs pratiques d'enregistrement. Dans le premier cas, la banque informe maintenant les clients au début de l'appel que leur conversation est enregistrée et leurs offrent des solutions de rechange pour communiquer leurs renseignements s'ils ne désirent pas poursuivre leur appel. Dans le deuxième cas, la banque a mis en place un message enregistré pour informer les clients que leur conversation sera enregistrée.

Un FAI tient en « otage » des messages électroniques

Une cliente s'est plainte lorsqu'elle a appris que son fournisseur d'accès Internet (FAI) continuait à recevoir et à stocker ses messages électroniques même si son compte était suspendu. Il s'agit là en réalité d'une pratique normale de l'industrie. Plusieurs FAI utilisent la réception et le stockage continus de messages électroniques comme un moyen pour aller chercher des paiements en retard.

Dans ce cas, l'ancien commissaire a déterminé que le FAI n'avait pas informé la plaignante de manière appropriée des fins liées à l'utilisation des renseignements personnels au cours de la suspension du compte et avait par conséquent utilisé ses renseignements personnels sans son consentement éclairé à des fins autres que celles pour lesquelles les renseignements avaient été recueillis. Compte tenu de ce fait, nous avons conclu que la plainte était fondée.

Mais ce cas a suscité une grande préoccupation pour le Commissariat au sujet de la pratique en question, que nous savions largement répandue dans l'industrie. Dans la lettre de conclusions, l'ancien commissaire a émis le commentaire suivant :

> *« ... en tant que commissaire à la protection de la vie privée, je demeure préoccupé au sujet des conséquences que peut avoir la pratique qui consiste à stocker et à conserver des messages potentiellement importants sans informer le destinataire prévu ni de leur existence ni l'expéditeur de leur défaut de livraison. Étant moi-même un utilisateur occasionnel des messages électroniques, au lieu de me laisser croire faussement que le message est passé sans obstacle, j'aimerais bien mieux que le message me soit retourné avec un avis indiquant qu'il n'a pas pu être livré, pour que je puisse ainsi rejoindre le destinataire prévu par d'autres moyens. En réalité, le fait de retourner le message accompagné d'un avis me semble la mesure la plus appropriée et la plus responsable à prendre de telles circonstances pour un fournisseur d'accès Internet. »* [traduction]

Afin donc de répondre à la question soulevée ci-dessus, un FAI devrait suivre, dans les cas d'une suspension de compte, ce nous avons recommandé comme pratiques exemplaires dans le cas en question :

- Cesser la collecte, le stockage et le refus d'accès aux messages électroniques destinés aux détenteurs des comptes suspendus.
- Adopter plutôt une pratique qui consiste à détourner les messages électroniques et à les retourner aux expéditeurs accompagnés d'un avis les informant que le message n'a pu être délivré.
- Prendre des dispositions pour donner accès au détenteur d'un compte suspendu à tous les messages électroniques reçus par l'entreprise, mais qui n'avaient pas été récupérés par le client au moment de la suspension.

Assurez-vous de vérifier ces pouvoirs qu'invoque le gouvernement

Les souvenirs de vacances d'une personne ont été gâchés lorsqu'elle a découvert que le transporteur aérien avec lequel elle avait effectué son voyage avait communiqué son itinéraire à son employeur. Son employeur, un ministère du gouvernement fédéral, menait une enquête qui portait sur l'utilisation du congé de maladie du plaignant. Le ministère a demandé au transporteur aérien de confirmer certains renseignements sur l'itinéraire de son voyage.

Le transporteur aérien a hésité. Invoquant ses obligations en vertu de la *LPRPDÉ*, il a demandé au ministère une preuve attestant que le plaignant avait donné son consentement à une telle communication. Si cela n'était pas possible, le transporteur aérien a suggéré qu'une exemption ou une exception spécifique en vertu de la *Loi* serait nécessaire pour lui permettre de satisfaire à la demande.

En réponse à cette suggestion, le ministère a invoqué une directive en vertu du pouvoir conféré par une loi fédérale particulière, indiquant que les renseignements étaient nécessaires aux fins de l'administration de la loi régissant l'emploi des fonctionnaires fédéraux et a demandé au transporteur

aérien de lui communiquer l'itinéraire du plaignant. Convaincu que la demande du ministère était conforme à l'aliéna 7(3)(*c*.1)(iii) de la *Loi*, le transporteur aérien a dûment communiqué les renseignements. Cet alinéa permet à une organisation de communiquer des renseignements au sujet d'une personne à une institution gouvernementale à des fins d'administration de la loi.

Il y avait cependant un seul problème. Le ministère n'a pas invoqué la bonne directive comme autorité légitime. Même si par la suite le ministère a reconnu son erreur, il a maintenu qu'il avait tout de même l'autorité légitime de recueillir ces renseignements en vertu d'une autre loi.

Nous avons convenu que le ministère avait l'autorité légitime. Toutefois, nous étions préoccupés par le fait que le ministère avait commis une erreur au départ et que le transporteur aérien avait omis de vérifier l'exactitude de l'autorité invoquée par le ministère. Même si le transporteur aérien a communiqué les renseignements de bonne foi, une organisation a l'obligation d'être vigilante en ce qui a trait à la vérification des pouvoirs invoqués par les organisations gouvernementales avant de communiquer des renseignements personnels. Dans sa lettre de conclusions, l'ancien commissaire a déclaré à ce propos :

> *« ...dans les cas de demandes de communication de renseignements personnels, je considère qu'il revient à toute organisation du secteur privé de ne pas accorder foi de prime abord aux demandes d'une organisation gouvernementale, mais plutôt d'être vigilante en ce qui a trait à la vérification des pouvoirs invoqués. »* [traduction]

Frais d'accès : devriez-vous payer pour avoir accès à vos propres renseignements?

Le fait de répondre à des demandes d'accès aux renseignements personnels peut occasionner des coûts pour une organisation. Cela devrait-il occasionner également des coûts pour les personnes? En réalité, il existe une disposition dans la *Loi* qui permet aux organisations d'imposer des droits

lorsqu'elles répondent aux demandes. Mais quels montants sont considérés comme étant raisonnables? Cette question a été traitée dans deux cas où les plaignants accusaient les organisations d'imposer des droits excessifs.

Ces deux cas représentent un bon exemple de la manière dont le secteur privé s'adapte aux attentes de la Loi.

Les plaignants étaient impliqués dans des disputes avec leur banque respective concernant un prêt qu'ils avaient contracté. Les deux personnes ont demandé à avoir accès à leurs renseignements personnels. Les banques ont répondu en leur exigeant des droits de 150 $ et de 200 $ respectivement, afin de couvrir les coûts de traitement des documents en question. La première personne voulait savoir ce qu'elle allait obtenir pour son argent et lorsqu'elle en a été informée, elle a décidé de porter plainte. La deuxième personne perçoit un revenu fixe et ne pouvait se permettre de payer un tel montant pour obtenir ses renseignements personnels.

Ces deux cas représentent un bon exemple de la manière dont le secteur privé s'adapte aux attentes de la *Loi*. On a rappelé aux banques que le principe 4.9.4 de la *LPRPDÉ* stipule qu'une organisation qui reçoit une demande de communication de renseignements personnels doit y répondre et ne peut exiger, pour ce faire, que des droits minimes. Cela a eu pour effet qu'une des banques a accepté de communiquer les renseignements à aucun frais, tandis que l'autre a imposé des frais nominaux de 10 $.

De plus, la position de la banque dans le cas du premier plaignant semblait être basée non seulement sur une question de recouvrement des coûts, mais également sur son désir de rencontrer le client afin de discuter de la dispute qui avait donné lieu au départ à la demande d'accès aux renseignements. Cependant, nous avons signifié à la banque que la *Loi* n'exige pas qu'une personne explique les raisons pour lesquelles elle souhaite avoir accès à ses

renseignements personnels ni qu'elle ait une discussion avec l'organisation concernant ses raisons. En d'autres termes, les renseignements personnels ne peuvent être mis à rançon.

Compte tenu de ces conclusions, la consigne essentielle pour les organisations en ce qui concerne les droits est celle-ci : le recouvrement des coûts ne s'applique pas aux demandes d'accès à l'information.

Une autorisation de sécurité devient une condition d'emploi

La protection des sites nucléaires contre les attaques terroristes est l'objet d'une sérieuse préoccupation surtout depuis le 11 septembre 2001. L'organisme fédéral qui supervise les opérations de toutes les installations nucléaires au Canada a répondu à la menace terroriste en ordonnant à ces titulaires de permis de mettre en œuvre des mesures de sécurité améliorées. L'une des nouvelles mesures en place consiste à limiter l'entrée aux installations nucléaires aux personnes ayant l'autorisation de sécurité appropriée. Si un titulaire de permis refuse de se conformer à cette nouvelle mesure, l'organisme fédéral révoquera sa licence de production.

Une division des produits nucléaires de l'entreprise a informé ses employés de la nouvelle exigence en matière de sécurité et leur a également demandé de consentir à une vérification de sécurité. Chaque employé de la division a reçu une trousse d'information accompagnée de formulaires de consentement qui précisaient le type de renseignements qui seraient recueillis, le but de la collecte et le nom de l'agence responsable de la collecte. Les employés ont aussi été informés que l'agence chargée de la collecte des renseignements personnels était liée par une entente concernant la confidentialité.

Afin d'obtenir une autorisation de sécurité, les employés comptant plus de dix ans de service devaient satisfaire à une vérification du casier judiciaire. Les employés comptant moins de dix ans de service devaient satisfaire à une vérification complète de leurs antécédents, notamment les antécédents en matière d'emploi, les compétences professionnelles et les références personnelles, ainsi qu'à la vérification de leur casier judiciaire.

Certains employés était mécontents et se sont plaints au Commissariat. Ils avaient l'impression de n'avoir aucun autre choix – s'ils refusaient, ils perdaient leur emploi. S'ils y consentaient mais qu'ils ne satisfaisaient pas à la vérification de sécurité, ils perdraient leur poste actuel et seraient réaffectés éventuellement à des postes moins bien payés. Ils avaient le sentiment, dans ces circonstances, que leur consentement était forcé.

L'ancien commissaire devait déterminer si l'entreprise avait recueilli les renseignements personnels de ses employés après les en avoir informés et obtenu leur consentement en vertu du principe 4.3 de la *LPRPDÉ*. Il était clair que les employés étaient au courant de cette collecte. Mais leur consentement était-il volontaire? Dans ses lettres de conclusions, l'ancien commissaire a jaugé la question de la façon suivante :

> *« [l'entreprise] vous a expressément demandé de donner votre consentement et il n'appartenait qu'à vous de le faire ou non. Le fait qu'il peut en découler des conséquences négatives dans l'un ou l'autre cas ne change rien au fait qu'on vous avait offert un choix en l'espèce. Le fait de refuser de consentir à la collecte de renseignements personnels peut très souvent entraîner des conséquences négatives pour la personne. Mais dans ce cas, comme dans la plupart des décisions prises dans la vie qui risquent d'avoir des conséquences négatives, la pression que vous pouvez ressentir au sujet du consentement à donner dans le cadre de la collecte ne constitue pas une contrainte. En vertu de la* Loi, *la principale considération n'est pas de savoir si des conséquences négatives peuvent découler ou non du refus d'une personne de donner son consentement, mais plutôt de savoir si la collecte est elle-même raisonnable ou non.* » [traduction]

Était-il raisonnable de recueillir des renseignements personnels à des fins d'autorisation de sécurité, comme stipulé au paragraphe 5(3) de la *Loi*? L'ancien commissaire a conclu qu'il était entièrement raisonnable de la part de l'organisme fédéral d'imposer à ses titulaires de permis des exigences accrues en matière de sécurité, compte tenu des préoccupations considérablement aiguës au sujet d'éventuels actes de terrorisme dans les installations nucléaires. Si l'entreprise ne s'était pas conformée à la directive de l'organisme fédéral, elle aurait perdu sa licence de production de

combustibles nucléaires et n'aurait plus été en mesure de poursuivre ses activités liées aux produits nucléaires, ce qui aurait entraîner des pertes financières considérables et des mises à pied. Dans ces circonstances, nous avons déterminé qu'il était entièrement raisonnable de la part de l'entreprise de se conformer à la directive et, ce faisant, de recueillir des renseignements personnels auprès des employés afin d'effectuer des vérifications de sécurité.

Aéroplan : l'option de refus n'est pas suffisant

Lorsque Air Canada a envoyé par la poste des brochures sur la la protection des renseignements personnels à 60 000 membres Aéroplan, plusieurs ont déposé une plainte au Commissariat.

Les personnes qui se sont plaintes au Commissariat n'étaient pas du tout contrariées par l'effort entrepris par la compagnie dans le but d'obtenir leur consentement à propos des pratiques de partage d'information en vertu du programme Aéroplan. Elles s'opposaient toutefois à ce qu'on rejette sur *elles* la responsabilité d'informer Air Canada si elles *ne* consentaient *pas* aux pratiques énoncées dans la brochure. Elles n'appréciaient pas non plus que l'entreprise présume, dans l'intervalle, qu'elles y consentaient.

L'ancien commissaire a conclu qu'Air Canada ne s'est pas conformé pas à la *LPRPDÉ* et que les plaintes étaient fondées.

Les 60 000 brochures ne représentaient qu'environ un pour cent du nombre total de membres Aéroplan à ce moment. Dans ses lettres de conclusions, l'ancien commissaire a fait remarquer que la *Loi* exige que les organisations respectent les droits à la vie privée de chaque personne et ne permet pas une conformité de pure forme. Étant donné qu'Air Canada avait en fait laissé 99 p. 100 des membres Aéroplan dans l'ignorance au sujet de sa politique et de ses pratiques de partage d'information, l'ancien commissaire a jugé que la démarche que la compagnie a entreprise dans le but d'obtenir ce consentement avait été entièrement inadéquate.

Même si tous les membres du programme avaient été consultés, la brochure même n'utilisait pas une formule de consentement appropriée. Elle décrivait cinq

façons dont Air Canada comptait partager les renseignements personnels des membres Aéroplan dans le cadre du programme. Chaque description était accompagnée d'une case à cocher et le membre du programme devait cocher la case seulement s'il ne consentait pas à ce que ses renseignements personnels soient partagés de la manière décrite. Tout membre du programme qui cochait une ou plusieurs des cinq cases devait ensuite retourner la brochure par la poste à l'entreprise afin de signifier le refus de consentement. Inversement, tout membre du programme qui ne retournait pas la brochure était considéré comme un membre ayant consenti aux cinq façons de partager l'information.

À l'instar de la plupart des autres personnes impliquées dans la protection de la vie privée et, en fait, comme la plupart des consommateurs avertis, nous avons une très mauvaise opinion de l'abonnement par défaut qu'utilisent les organisations pour le traitement des renseignements personnels.

Cette forme de consentement est à présent connue sous le nom de « consentement négatif » ou « option de refus ». Elle correspond aux pratiques de marketing de l'« abonnement par défaut » que les consommateurs ont vite fait de condamner dans le passé. En effet, une telle pratique est fondée sur la présomption – la personne est présumée donner son consentement à moins qu'elle n'entreprenne des démarches pour le refuser.

À l'instar de la plupart des autres personnes impliquées dans la protection de la vie privée et, en fait, comme la plupart des consommateurs avertis, nous avons une très mauvaise opinion de l'abonnement par défaut qu'utilisent les organisations pour le traitement des renseignements personnels. Le Commissariat considère que l'option de refus est une forme médiocre de

consentement, qui rejette injustement la responsabilité sur le mauvais parti et reflète au mieux un respect de pure forme de ce qui est sans doute le principe le plus fondamental de la *Loi*. Nous préférerions que les organisations adoptent une approche exclusivement positive ou fondée sur l'« option d'acceptation » – une approche beaucoup plus respectueuse selon laquelle on estimerait qu'une personne a consenti seulement si elle a catégoriquement dit « oui » à une proposition.

Par ailleurs, le Commissariat est aussi conscient que l'option de refus est une forme de consentement expressément permise par la *Loi* dans certaines circonstances – notamment, lorsque les renseignements personnels sont manifestement de nature non sensible. Le problème dans ce cas est que la *Loi* ne définit pas précisément la notion de sensibilité. Bien qu'elle énonce que les renseignements financiers et médicaux d'une personne doivent presque toujours être considérés comme étant sensibles, elle suggère que n'importe quel renseignement peut être sensible selon le contexte. Par conséquent, en ce qui concerne les plaintes relatives à Aéroplan, la tâche du Commissairait consistait essentiellement à évaluer le contexte. Autrement dit, l'ancien commissaire devait déterminer si les circonstances justifiaient le recours par Air Canada à l'option de refus.

Dans ses lettres de conclusions, l'ancien commissaire a expressément fait état de son intention de toujours établir de limites strictes en ce qui concerne les circonstances dans lesquelles l'option de refus pourrait être jugée appropriée. Il a aussi clairement exprimé son intention de se laisser guider dans de telles délibérations par la prise en compte en bonne et due forme de la sensibilité des renseignements et des attentes raisonnables de la personne. C'est sur la base de ces considérations que la brochure d'Aéroplan sur la protection des renseignements personnels s'est avérée non conforme à la *Loi*.

Le libellé de la brochure ne montre pas que les situations de partage de l'information décrites étaient strictement de nature non sensible ou d'un contexte non sensible. Deux des situations étaient particulièrement sensibles. Les trois autres semblaient par leur description permettre un marketing de grande envergure à l'endroit des membres en fonction de renseignements

personnalisés suivant des critères de nature potentiellement sensible. L'ancien commissaire a ainsi déclaré dans ses lettres :

> *« Bien que je considère que la pratique qui consiste à partager les renseignements des membres du programme à des fins de publicité de produits, de services et de promotions spéciales soit en elle-même acceptable, je suis persuadé qu'une personne raisonnable ne s'attendrait pas à ce qu'une telle pratique s'étende à la « fabrication sur mesure » de l'information suivant les intérêts, les usages et les préférences de nature potentiellement sensible de la personne sans son consentement explicite. »* [traduction]

L'ancien commissaire a conclu qu'il avait été inapproprié pour Air Canada de recourir au consentement négatif ou à l'option de refus dans le cadre des politiques et des pratiques de partage d'information d'Aéroplan, telles que décrites dans la brochure.

À son honneur, Air Canada a pris très au sérieux les conclusions et les recommandations de l'ancien commissaire. Grâce à quelques conseils apportés par le Commissariat dans un processus qui nous a semblé à la fois positif et fructueux, la compagnie a entrepris de repenser et de ré-écrire sa politique de partage d'information dans le cadre d'Aéroplan. Nous avons examiné le produit fini et vérifié que la politique traite à présent de nos préoccupations des façons suivantes :

- elle explique aux membres Aéroplan, en termes clairs et compréhensibles, les buts de la collecte, de l'utilisation et de la communication des renseignements personnels dans le cadre du programme ;
- elle explique clairement qu'Aéroplan ne recueille aucun renseignement sur les opérations en fonction desquelles les membres accumulent des points dans le cadre du programme ;
- elle précise qu'Aéroplan ne fournit pas de profil personnalisé des membres aux entreprises partenaires ou à d'autres tierces parties, et précise également que tout renseignement fourni aux partenaires ne peut être utilisé qu'à des fins liées au programme Aéroplan ;

- elle énonce explicitement et clairement que les membres qui souhaitent que leurs renseignements personnels ne soient utilisés que pour le rachat de leurs points Aéroplan peuvent le stipuler et il fournit aux membres une méthode facile pour exercer cette option.

En ce qui concerne la question relative à la consultation de tous les membres Aéroplan, Air Canada a aussi dressé un plan très précis selon lequel tous les membres actifs du programme recevraient copie de la politique révisée avec leur prochain état de compte. De plus, la politique allait être affichée sur le site Web d'Aéroplan.

Nous étions convaincus qu'Air Canada avait répondu de façon appropriée à nos recommandations et nous sommes heureux de l'esprit de coopération dont l'entreprise a fait preuve.

Un cas de superchérie

C'est une chose de peu informer les personnes des fins pour lesquelles leurs renseignements personnels pourraient être utilisés, tel que l'ont fait trois des organisations mentionnées plus haut. C'est une autre chose de mal les informer de façon délibérée, tel que nous l'avons conclu dans le cas d'une plainte à l'encontre d'une entreprise d'études de marché.

Cette entreprise envoie par la poste des questionnaires pour ce qu'elle appelle des « sondages sur des produits grand public » aux ménages à travers le Canada. Les questionnaires comportent des questions sur les présences des ménages parmi diverses catégories de produits. La documentation qui accompagne les questionnaires explique les objectifs du sondage strictement en terme de recherche des « faits », de collecte « d'opinions » et de compréhension des « préférences et des attitudes des consommateurs », le tout dans le but d'améliorer la qualité, la durée et la valeur des produits.

Cependant, les sondages avaient réellement pour objectif de vendre des produits aux répondants du sondage. Ce que l'entreprise avait principalement l'intention de faire avec les renseignements qu'elle recueillait était de compiler les listes d'envoi personnalisées qui, par la suite, seraient données aux tierces

parties qui avaient commandé le sondage en question. Celles-ci essayeront par la suite de vendre leurs produits aux répondants du sondage en leur envoyant directement de la publicité en fonction des renseignements qu'ils ont fournis dans les réponses aux questionnaires.

Si une organisation a l'intention de transmettre les renseignements qu'elle recueille directement à des commerçants, elle doit le mentionner...

La *LPRPDÉ* stipule qu'une organisation doit énoncer les vrais motifs pour lesquels elle recueille des renseignements personnels. Elle stipule également que le consentement à la collecte de renseignements personnels ne doit pas être obtenu par une supercherie.

Si une organisation a l'intention de transmettre les renseignements qu'elle recueille directement à des commerçants, elle doit le mentionner, en termes clairs et énoncés de façon à être raisonnablement compris par les personnes. Dans la documentation du sondage en question, il n'existe aucune déclaration explicite ni une aucune insinuation compréhensible et raisonnable informant les répondants que leurs renseignements personnels seraient communiqués à des tierces parties.

Le questionnaire sollicite le consentement des répondants en vue d'autres envois et offres postaux, mais ne mentionne pas de quelles sources proviendront ces envois. En l'absence de telle indication mentionnant que l'entreprise de sondages a l'intention de partager l'adresse postale du répondant avec d'autres expéditeurs éventuels, l'inférence la plus raisonnable serait que tous les envois et les offres proviendront de la même source que celle qui était à l'origine de la collecte, c'est-à-dire de l'entreprise de sondages elle-même.

De plus, la formule de consentement pose en elle-même un problème. Compte tenu du fait que les questions du sondage sont de nature hautement

sensible (en l'occurrence, plusieurs questions concernent la santé et les finances personnelles), la formule de consentement de l'« option d'acceptation » devrait être utilisée dans de telles circonstances. Mais la formule de consentement consiste à cocher une des deux cases, « Oui » et « Non », ce qui rend plutôt ambiguë la formule de consentement recherchée. Cependant, ce qui se passe en réalité, dans les cas assez fréquents où le répondant ne coche aucune des cases, c'est qu'on présume que la personne consent à recevoir d'autres envois. Ainsi, l'entreprise utilise la formule de consentement de l'« option de refus » dans une situation qui fait clairement appel à une « option d'acceptation ».

La documentation du sondage mentionne également que des entreprises ont commandé ce sondage. Cependant, elle ne nomme pas ces entreprises, ni ne suggère de façon perceptible que ces entreprises anonymes sont des agences de vente directe ou qu'ils ont en effet commandé à l'entreprise d'études de marché ce sondage dans le but de recueillir des renseignements personnels sur d'éventuels consommateurs. En réalité, il n'existe rien dans la documentation qui pourrait donner aux ménages des raisons de croire que le sondage n'est rien d'autre de ce qu'il prétend être à première vue, c'est-à-dire une étude de marché axée sur la recherche de faits et d'opinions, qui vise à améliorer les produits.

En fonction d'une telle description, les répondants pourraient s'attendre à ce que les entreprises qui ont commandé le sondage en reçoivent les résultats sous forme de données analytiques cumulatives et anonymes. Mais les répondants n'ont aucune raison légitime de s'attendre, et ils ont toutes les raisons d'en être insultés, à ce que leur participation au sondage ait pour effet de les rendre sujets à des efforts de marketing direct non désirés qui portent atteinte à la protection de leur vie privée par des tierces parties qui ont eu connaissance de renseignements personnels de nature sensible les concernant.

Cela peut sembler paradoxale pour certains que, malgré le cas accablant contre l'entreprise d'études de marché en raison de ces allégations et de bien d'autres, nous étions principalement préoccupés par les signes évidents de la *conformité* de l'entreprise avec la *Loi*.

En réalité, l'entreprise a une politique officielle écrite, affichée sur son site Web, sur la protection des renseignements personnels concernant ses sondages effectués auprès des ménages. Cette politique détermine relativement bien les fins réelles de la collecte des renseignements de sondage. Cependant, cette politique n'est non seulement pas intégrée à la documentation du sondage envoyée par la poste aux ménages, mais elle n'est pas non plus accessible de façon raisonnable aux ménages. La documentation du sondage ne mentionne même pas l'existence du site Web, encore moins l'existence de cette politique.

Ce qui nous a troublés particulièrement était le grand écart concernant la conformité avec la *Loi*, entre le site Web et la documentation du sondage, ainsi que les conséquences de cet écart. Dans la lettre de conclusions, l'ancien commissaire a soulevé les préoccupations suivantes :

> « *Pourquoi [l'entreprise] indiquerait-elle de manière raisonnablement claire dans une politique sur la protection des renseignements personnels, tenue à l'écart et non annoncée, mais de façon nébuleuse dans la documentation sur le sondage remise aux personnes, que les renseignements personnels des répondants seraient communiqués à des tierces parties à des fins de marketing? Pourquoi dans les documents de sondage, [l'entreprise] explique-t-elle les fins en des termes aussi restreints que la recherche de faits, la collecte d'opinions et l'amélioration de la qualité des produits et relègue dans un document, dont personne ne pourrait normalement prendre connaissance, les autres fins de marketing direct par des tierces parties? En réalité, pourquoi [l'entreprise] ferait l'effort de formuler une politique en matière de protection de renseignements personnels plus ou moins conforme à la* Loi *pour ne pas attirer ensuite l'attention de chaque répondant à cet égard au moment où cela importe réellement, en cachant, de fait, la politique aux consommateurs.*[2] » [traduction]

> « *En résumé, j'ai de la difficulté à comprendre cet écart, excepté en termes de supercherie. [L'entreprise] a suggéré que ses documents de sondage servaient à susciter une attente raisonnable de communication aux tierces parties et de marketing direct de leur part. Cependant, je ne comprends pas comment une personne peu méfiante pourrait supposer une telle fin à partir des indications*

insuffisantes, vagues et trompeuses qui lui sont fournies. Au lieu de cela, de mon point de vue, loin d'offrir une compréhension raisonnable de la manière dont les renseignements personnels seront utilisés ou communiqués, les documents du sondage ont uniquement servi à tromper les personnes sur les véritables objectifs des sondages et à nuire à l'équité de la collecte des renseignements personnels par l'entreprise. » [traduction]

Un groupe d'intérêt propose des « attentes » en matière de consentement

La *LPRPDÉ* stipule, au principe 4.3.5 de l'annexe 1, que les attentes raisonnables de la personne sont pertinentes en matière de consentement. Mais elle n'approfondit pas le sujet.

Elle nous laisse plutôt la tâche ardue d'interpréter cette disposition. Dans le contexte de toute plainte liée au consentement, il revient souvent au commissaire de déterminer le caractère raisonnable des attentes du plaignant, ainsi que leur portée réelle. Heureusement, dès l'entrée en vigueur de la *Loi*, une série de plaintes ont été portées de sorte que nous avons jugé utile de formuler une position générale sur ce qu'une personne devait s'attendre en matière de consentement.

Une personne a déposé une plainte au nom d'un groupe d'intérêt à l'encontre deux banques, une compagnie de télécommunications et une entreprise qui offre un programme pour les clients réguliers. Toutes les plaintes étaient relativement semblables et alléguaient que les organisations en question n'avaient pas obtenu de consentement valide et informé auprès des personnes pour communiquer à des fins de marketing des renseignements personnels les concernant.

Les plaintes consistaient en deux allégations principales. Selon la première, les organisations ne faisaient pas d'efforts raisonnables pour informer leurs clients que leurs renseignements personnels pourraient être communiqués à des tierces parties à des fins secondaires de marketing, c'est-à-dire à des fins en sus de celles pour lesquelles il a été nécessaire de recueillir les renseignements au départ. Le plaignant a allégué que si les personnes n'étaient pas dûment

informées des fins secondaires, les organisations n'avaient aucune base valide de présumer le consentement des personnes à de telles fins. Selon la seconde allégation, en dépit du fait qu'elles se fiaient à la formule de consentement de l'option de refus, les organisations n'offraient pas aux personnes des possibilités raisonnables d'exercer l'option de refus dans le cadre du marketing mené par les tierces parties.

Pour nous, ces suppositions traduisaient clairement des « attentes » de la part du plaignant.

Aussi intéressantes que les allégations elles-mêmes furent les suppositions sous-jacentes que le groupe d'intérêt avait présentées dans une déclaration de principe soutenant les plaintes. Pour nous, ces suppositions traduisaient clairement des « attentes » de la part du plaignant. Avant de déterminer si les organisations en question s'étaient conformées ou non aux dispositions pertinentes de la *Loi* sur le consentement, nous avons jugé qu'il est prudent d'examiner la question de savoir si les attentes du groupe au sujet du consentement étaient elles-mêmes raisonnables au regard de la *Loi*.

Après les avoir analysées, l'ancien commissaire a conclu que les attentes du groupe étaient entièrement raisonnables. Plus particulièrement, il a jugé qu'il est raisonnable d'attendre des organisations qui utilisent ou qui communiquent des renseignements personnels à des fins secondaires ce qui suit :

- Ce n'est pas assez de déterminer des objectifs dans des documents portant sur la politique en matière de protection des renseignements personnels et de les rendre largement disponibles. Une organisation devrait porter ses fins secondaires directement à l'attention de la personne au moment de recueillir les renseignements personnels. À l'occasion d'une demande ou d'un abonnement, par exemple, la personne devrait recevoir les renseignements nécessaires et on ne devrait pas lui référer des sources qui ne sont pas immédiatement disponibles. (Ces attentes sont soutenues par

les principes 4.2.3 et 4.3.1 de la *Loi*, qui stipulent que la détermination des fins et l'obtention du consentement soient directes et coïncident avec la collecte des renseignements personnels).

- Les fins devraient être stipulées dans un langage clair, simple et compréhensible pour le consommateur ordinaire et de façon bien détaillée afin que celui-ci puisse apprécier la nature et l'étendue de la collecte, de l'utilisation et de la communication envisagées. (Ces attentes sont soutenues par le principe 4.3.2, qui stipule que les fins doivent être énoncées de telle façon que la personne puisse de manière raisonnable comprendre de quelle manière les renseignements seront utilisés ou communiqués).
- Si les fins sont déterminées par écrit, la personne ne devrait pas être obligée de les lire en caractères minuscules dans des passages denses.

Lorsqu'une organisation a l'intention de présumer le consentement d'une personne à des fins secondaires, elle devrait offrir aux personnes la possibilité d'exercer l'option de refus. La possibilité et la procédure d'option de refus devraient vraisemblablement être portées à l'attention de la personne au moment de la collecte de renseignements personnels. La procédure d'option de refus devrait être simple, immédiate et peu coûteuse.

Compte tenu de ces éléments et après enquête sur les politiques et les pratiques réelles des organisations, l'ancien commissaire a conclu que deux des plaintes étaient fondées et que deux ne l'étaient pas. Il a conclu que la compagnie de télécommunications ne communiquait aucun renseignement tel qu'allégué, puisque le CRTC l'interdit. L'une des banques communiquait effectivement des renseignements à des fins secondaires de marketing tel qu'allégué, mais l'ancien commissaire a conclu que la banque faisait dans l'ensemble des efforts raisonnables pour informer les personnes désirant ouvrir un compte de la pratique, pour obtenir leur consentement et pour leur offrir une possibilité d'exercer l'option de refus.

Dans le cas des plaintes fondées, la non conformité avec la *Loi* du programme pour clients réguliers était largement due à une incohérence des procédures d'inscription. Cependant, le cas de la seconde banque était plus sérieux. Les

efforts entrepris par la banque pour obtenir un consentement éclairé auprès des personnes désirant ouvrir un compte ne satisfaisaient aucunement aux exigences de la *Loi* ni les attentes raisonnables de la personne. Dans la lettre de conclusions, l'ancien commissaire a émis des commentaires sur divers documents utilisés par la banque afin de communiquer ses fins, ainsi que sur la nature et la portée du non respect de la *Loi* dans ce cas :

> *« Les termes ... sont tellement vagues qu'ils sont presque incompréhensibles, à moins qu'on les interprète comme voulant dire que la banque a l'intention d'utiliser les renseignements personnels comme bon lui semble et de les communiquer à qui elle veut. Ce qui constituerait à peine une fin à laquelle aucune personne raisonnable ne s'attendrait et qu'aucune personne raisonnable ne jugerait appropriée en aucun cas.* » [traduction]

En revanche, sur une note positive, on devrait noter que, dans le cas de la première banque, l'ancien commissaire a complimenté la banque sur son approche concernant l'obtention du consentement éclairé de la part des personnes désirant ouvrir un compte. Dans le cas des personnes faisant une demande directement dans une succursale, la procédure de demande de cette banque exige que l'on s'asseye avec la personne, qu'on lui donne immédiatement les renseignements appropriés sur la protection des renseignements personnels, que l'on attire son attention particulièrement sur les déclarations concernant les fins secondaires de marketing, qu'on lui demande si elle consent ou non à des pratiques de marketing particulières, que l'on prenne note de ses réponses et qu'on les respecte. Nous considérons de telles procédures comme exemplaires, presque autant que la forme positive de consentement que nous préférons.

Consentement à des fins secondaires

Ce qui suit constitue un sommaire des délibérations menées jusqu'à ce jour dans des cas relatifs au consentement à des fins secondaires :

- Le consentement positif ou actif doit toujours être préféré comme la forme de consentement la plus forte, la plus respectueuse des personnes et la

meilleure pour rester fidèle à l'esprit de la *Loi*. On encourage fortement les organisations à adopter exclusivement cette forme de consentement.

- Le consentement positif ou actif à des fins secondaires est nécessaire dans des situations où les renseignements personnels sont de nature sensible ou dans des situations où il existe une grande probabilité pour que les renseignements deviennent de nature sensible dans le contexte des activités de gestion des renseignements.

- Puisque la *Loi* indique que les renseignements personnels de nature financière ou médicale doivent presque toujours être considérés comme étant de nature sensible, on présume que ces types de renseignements devront presque toujours exiger un consentement positif. Cependant, puisque la *Loi* stipule également que tout renseignement personnel peut être de nature sensible dans un contexte donné, aucune autre tentative ne devrait être faite pour définir précisément la notion de sensibilité. Le contexte devrait plutôt être considéré dans chaque cas dans le but de déterminer le potentiel de sensibilité.

- Les deux principales considérations permettant de déterminer le potentiel de sensibilité des renseignements personnels sont l'intention de communiquer les renseignements à des tierces parties et l'intention de classer ou autrement dit de traiter les renseignements selon des critères personnels.

- Le consentement négatif ou passif, également connu sous le nom de consentement présumé, même si celui-ci représente la forme la plus faible et la moins préférable, est reconnu en vertu de la *Loi* comme étant acceptable dans certaines circonstances. La portée des circonstances dans laquelle cette forme de consentement est permise demeure limitée.

- L'utilisation par une organisation de la forme négative ou passive de consentement à des fins secondaires sera justifiée seulement sous les conditions suivantes :

    - Les renseignements personnels doivent s'avérer, démonstration faite, de nature et d'un contexte non sensible et doivent être déterminés par élément ou par catégorie.

- Si les renseignements doivent être communiqués à des tierces parties, les parties doivent être identifiées par nom ou par catégorie.
- L'organisation doit stipuler ses fins en se conformant entièrement aux principes 4.2, 4.2.3, 4.3.1 et 4.3.2 et aux attentes raisonnables de la personne jugées pertinentes en vertu du principe 4.3.5. Plus particulièrement, les fins déterminées doivent être directement portées à l'attention de la personne, oralement ou par écrit, au moment de la collecte de renseignements personnels (par exemple, lors du processus d'abonnement, de demande ou d'inscription) ; en termes clairs, précis et sans équivoque ; dans un format facile à lire (lorsqu'il s'agit d'un texte) ; et d'une façon permettant à la personne de comprendre de quelle manière exactement les renseignements personnels seront utilisés ou communiqués.
- L'organisation doit offrir une formule d'option de refus appropriée, c'est-à-dire une possibilité et une procédure convenables pour retirer un consentement. La formule doit être expliquée à la personne au moment de la collecte de renseignements personnels à son sujet et devrait être peu coûteuse, facile à exécuter et avec effet immédiat quant au retrait du consentement. Si possible, elle devrait comprendre un numéro de téléphone sans frais.

INCIDENTS VISÉS PAR LA *LPRPDÉ*

Vérification des appels téléphoniques

Un journaliste a communiqué avec le Commissariat au sujet d'un sondage qu'effectuait un cabinet de recherche pour le compte d'une compagnie de téléphone. Il a semblé que l'entreprise recueillait auprès des clients des renseignements à propos de leurs appels téléphoniques.

Le cabinet de recherche avait signé un contrat avec la compagnie de téléphone afin d'effectuer des vérifications au hasard à des fins d'assurance de la qualité. La compagnie de téléphone a fourni au cabinet une liste des numéros de téléphone de clients qui avaient téléphoné pour obtenir de l'assistance en composant le « 0 » ou le « 411 ». Le cabinet n'a pas reçu le

nom des clients ni d'autres renseignements pouvant les identifier. L'entreprise a signé un contrat de non-divulgation avec le cabinet, qui exigeait que le cabinet détruise tous les renseignements qu'il recueillait une fois que les résultats du sondage auront été compilés.

L'ancien commissaire était heureux d'apprendre qu'il a été déterminé que la compagnie de téléphone se conformait à une exigence du CRTC voulant que celle-ci mesure régulièrement la qualité du service relativement à l'exactitude des services de l'assistance-annuaire.

Trouvaille près d'une benne à ordures

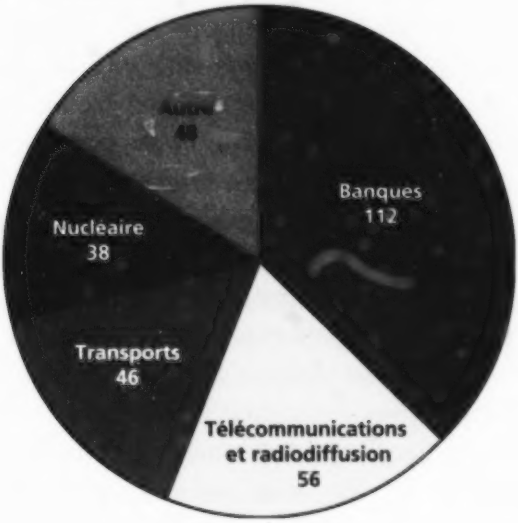
Une banque a alerté le Commissariat que des documents confidentiels sur des clients avaient été retrouvés dans une benne à ordures située près de la succursale qui avait fermé quelque temps auparavant. L'édifice avait été loué à un nouveau locataire et était en rénovation. Apparemment, les personnes qui effectuaient les rénovations avaient trouvé les documents au cours des travaux, puis les avaient jetés. Après avoir eu vent de l'incident, les médias ont récupéré certains documents de la benne à ordures.

La banque a réagi rapidement aussitôt qu'elle a pris conscience de la situation, en récupérant tous les documents qui se trouvaient dans la benne et ceux que les journalistes avaient entre les mains ; puis elle s'est assurée qu'il ne restait aucun autre document de la banque dans l'édifice. La banque a également informé tous les clients touchés, en personne ou par écrit, de l'incident et des mesures qu'elle avait prises pour récupérer les documents. De plus, la banque s'est excusée auprès de chaque client et leur a assuré que tous leurs renseignements avaient été récupérés.

Il a été déterminé que la succursale en question avait été fusionnée avec une autre succursale et qu'une entreprise privée sous contrat avec la banque avait été mandatée pour trier et traiter tous les dossiers. La banque a établi des procédures destinées à cet effet, mais l'entreprise privée ne les avait pas suivies correctement, ce qui a eu pour effet le fait que certains documents n'étaient pas bien classés et qu'ils avaient été jetés de façon inappropriée. La banque a par la suite clarifié les procédures avec l'entreprise privée.

L'ancien commissaire était convaincu que la banque avait réagi de manière rapide et appropriée face à cette situation délicate.

Nombre de plaintes selon le secteur
1er janvier 2002 au 31 décembre 2002



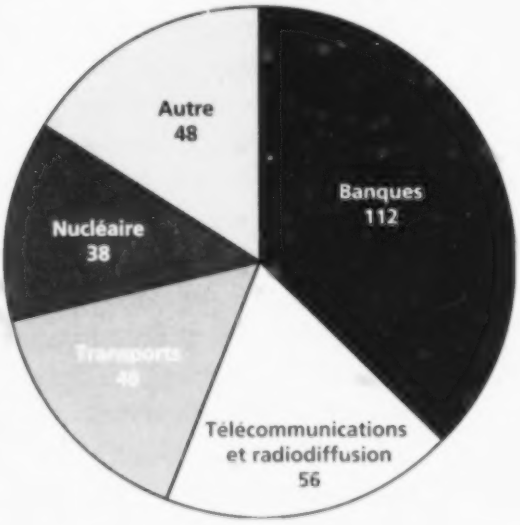
Demandes de renseignements en vertu de la *LPRPDÉ*
1er janvier 2002 au 31 décembre 2002 : 8 381

Nous essayerons de fournir une répartition de ces demandes de renseignements par thème dans les prochains rapports annuels

L'ancien commissaire était convaincu que la banque avait réagi de manière rapide et appropriée face à cette situation délicate.

Nombre de plaintes selon le secteur

1er janvier 2002 au 31 décembre 2002



Demandes de renseignements en vertu de la *LPRPDÉ*

1er janvier 2002 au 31 décembre 2002 : 8 381

Nous essayerons de fournir une répartition de ces demandes de renseignements par thème dans les prochains rapports annuels

EXAMENS ET PRATIQUES EN MATIÈRE DE VIE PRIVÉE

La *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*) autorise le commissaire à vérifier la conformité des organisations du secteur privé avec la *Loi* s'il a des motifs raisonnables de croire qu'elles contreviennent à la *Loi* ou qu'elles ne respectent pas une des recommandations énoncées dans l'annexe 1 (les dix principes). La Direction des examens et des pratiques en matière de vie privée du Commissariat effectuera des examens et des vérifications de conformité, aux termes de l'article 18 de la *LPRPDÉ*, en tenant compte des objectifs et des critères de vérification standard reconnus. Au cours de la période couverte par le présent rapport, un certain nombre de questions ont été portées à l'attention de l'ancien commissaire, qui ont été résolues avec succès sans qu'on n'ait eu besoin d'effectuer une vérification. Par exemple, le personnel du Commissariat a rencontré et conseillé des représentants d'une association d'entreprises sur la viabilité du consentement direct et le contenu proposé d'un tel formulaire de consentement. Nous avons offert des conseils à une entreprise en ce qui concerne l'utilisation du NAS comme identificateur et l'utilisation du consentement négatif. De plus, nous avons procédé à un examen et une analyse d'ensemble de la politique sur la protection des renseignements personnels d'une société.

Hormis ces questions, l'ancien commissaire n'a été au courant d'aucun autre problème qui aurait pu lui donner des motifs suffisants pour entreprendre une vérification en vertu de la loi.

Néanmoins, la Direction des examens et des pratiques en matière de vie privée a pris part à des consultations avec les organisations du secteur privé qui sont assujetties à la *LPRPDÉ* et leur a offert des conseils. Elle a également apporté son aide aux organisations qui ne sont pas régies par la *Loi* mais qui se préparent pour le 1er janvier 2004, lorsque la *Loi* commencera à s'appliquer à elles.

DEVANT LES TRIBUNAUX

Aux termes de l'article 14 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*), une personne ayant porté plainte a le droit, à l'issue de l'enquête du commissaire, de déposer une demande d'audience à la Cour fédérale du Canada sur toute question dont il est fait mention dans le rapport du commissaire. Ces questions doivent figurer parmi les clauses énoncées dans l'annexe, ainsi que dans les articles de la *LPRPDÉ*.

Aux termes de l'article 15 de la *LPRPDÉ*, le commissaire est autorisé à déposer une demande de comparution à la Cour fédérale. Il peut, avec le consentement du plaignant, demander directement une audience à la Cour sur toute question visée à l'article 14 ; comparaître devant la Cour au nom de tout plaignant qui a présenté une demande d'audience en vertu de l'article 14 ; ou, avec l'autorisation de la Cour, comparaître comme partie à une instance engagée en vertu de l'article 14.

Voici une liste des demandes déposées devant les tribunaux en vertu de la *LPRPDÉ* du 1er janvier 2001 jusqu'au 31 décembre 2002 :

Mathew Englander c. Telus Communications Inc.

N° de dossier de la Cour fédérale du Canada : T-1717-01

Il s'agit de la première demande qui a été déposée à la Cour fédérale aux termes de la *LPRPDÉ*. M. Englander soutient que Telus utilise et communique les noms, adresses et numéros de téléphone de ses clients figurant dans les pages blanches de son annuaire et ailleurs, à l'insu de ses clients et sans avoir obtenu leur consentement. En outre, Telus impose de manière inappropriée des frais aux clients qui demandent la « non-publication » de leur numéro de téléphone. M. Englander soutient que ces mesures prises par Telus sont contreviennent aux paragraphes 5(1) et (3) de la *LPRPDÉ*, ainsi qu'à plusieurs clauses de l'annexe 1 de la *Loi*.

État de la situation

Cette demande a fait l'objet d'un non-lieu le 2 juin 2003.

Ronald G. Maheu c. le procureur général du Canada et IMS Health Canada

N° de dossier de la Cour fédérale du Canada : T-1967-01

Ronald Maheu a demandé une audience à la Cour fédérale du Canada, soutenant qu'IMS Health Canada avait communiqué de manière inappropriée des renseignements personnels en vendant des données sur les habitudes de prescription des médecins sans avoir obtenu leur consentement.

État de la situation

M. Maheu a déposé un avis de demande modifié en mars 2002. IMS a présenté une requête demandant de soit rejeter la demande sur des motifs voulant que la demande ait été présentée à des fins inappropriées ou soit de demander à M. Maheu de verser une garantie pour les coûts. La Cour a ordonné à M. Maheu de déposer une garantie financière de 12 000 $ et a mentionné qu'elle avait des raisons de croire que M. Maheu utilisait la *Loi* à des fins accessoires et inappropriées, compte tenu du fait que ses propres renseignements personnels n'étaient pas en jeu. Lors de l'appel, l'ancien commissaire a comparu pour apporter son aide à la Cour relativement à l'interprétation adéquate de la *LPRPDÉ*, expliquant qu'une personne peut déposer une plainte concernant les pratiques de renseignements personnels d'une organisation sans égard au fait que celle-ci recueille, utilise ou communique des renseignements personnels la concernant. La Cour fédérale a accepté cette position et a accordé un appel à M. Maheu le 3 janvier 2003. Cette décision est actuellement en appel et la demande originale est encore traitée à la Section de première instance.

Diane L'Ecuyer c. Aéroports de Montréal

N° de dossier de la Cour fédérale du Canada : T-2228-01

Diane L'Ecuyer s'est plainte que les Aéroports de Montréal avaient envoyé des copies d'une lettre de réponse aux demandes d'accès qu'elle avait faites à deux représentants du syndicat et à un employé du coordinateur des relations et qu'ils avaient, par conséquent, communiqué des renseignements personnels à son sujet sans avoir obtenu son consentement. L'ancien

commissaire a fait enquêté sur sa plainte et recommandé dans ses conclusions que les personnes devraient être en mesure de juger par elles-mêmes si elles désiraient ou non partager une telle réponse avec les autres.

État de la situation

Madame L'Ecuyer a fait une demande à la Cour fédérale le 18 décembre 2001, demandant qu'une ordonnance soit formulée exigeant que l'organisation corrige ses pratiques pour se conformer à la *LPRPDÉ* et que l'organisation publie un avis mentionnant toutes les mesures prises ou proposées afin de corriger ses pratiques. La Section de première instance a rendu sa décision le 13 mai 2002 et conclu que la question s'est posée dans le cadre de l'administration d'une convention collective et que, par conséquent, le commissaire à la protection de la vie privée n'avait pas compétence dans cette cause. Madame L'Ecuyer a fait appel de la décision le 5 juin 2003 et le commissaire à la protection de la vie privée envisage demander une autorisation pour intervenir dans cet appel.

Nancy Carter c. Inter.net Canada Limited

N° de dossier de la Cour fédérale du Canada : T-1745-02

Nancy Carter a fait part de ces préoccupations au Commissariat concernant les pratiques d'un fournisseur d'accès Internet (FAI). Au cours d'une dispute concernant la facturation avec la plaignante, le FAI avait suspendu son accès à sa boîte de courrier électronique, mais le compte était toujours actif et acceptait les nouveaux messages électroniques dans la boîte aux lettres. La plaignante affirme qu'elle était ainsi donc privée d'accès à ses renseignements personnels, ce qui va à l'encontre de la *LPRPDÉ* et qu'elle a perdu des possibilités d'affaires précieuses à la suite de cet incident. Elle réclame donc un dédommagement en vertu de la *LPRPDÉ*.

État de la situation

Une entente a été conclue dans cette affaire et un avis d'abandon a été déposé le 5 juin 2003.

Sylvain Gagné c. Bell Canada

N° de dossier de la Cour fédérale du Canada : T-1971-02

Sylvain Gagné s'est plaint au Commissariat (a) du fait qu'on lui avait refusé l'accès à certains de ses renseignements personnels et (b) d'une communication inappropriée de renseignements personnels concernant d'autres personnes. Même si l'ancien commissaire a conclu que la plainte de refus d'accès était non fondée, en acceptant le fait que les exemptions en vertu de 7(1)*b*) et 9(3)*c*.1) avaient été correctement appliquées, la plainte sur la communication de renseignements personnels était fondée et l'ancien commissaire a formulé des recommandations concernant les changements à apporter aux pratiques.

État de la situation

L'avis de demande a été présenté à la Cour fédérale le 25 novembre 2002, demandant une série de dispenses, dont l'accès aux documents qui n'ont pas été communiqués, des dédommagements pour les personnes touchées et des ordonnances donnant pourvoir exécutoire aux recommandations.

Bell Canada a maintenant accepté de suivre les recommandations du Commissariat et un avis d'abandon a alors été déposé le 14 mars 2003.

Dale Stuart c. la banque Toronto Dominion

N° de dossier de la Cour fédérale du Canada : T-290-02

Dale Stuart croyait que des renseignements relatifs à ses affaires bancaires avaient été communiqués par des employés la banque TD à son employeur à son insu et sans son consentement.

État de la situation

Cette demande a été abandonnée par M. Stuart le 2 décembre 2002.

Société de l'hôpital du Yukon c. Solliciteur général du Canada

N° de dossier de la Cour fédérale du Canada : T-1814-02

Ce recours a été introduit en réponse à la détermination par l'ancien commissaire selon laquelle il avait compétence en vertu de l'alinéa 4(1)*b*) de faire enquête sur une plainte déposée à l'encontre de la Société de l'hôpital du Yukon.

État de la situation

Une plainte a été déposée au Commissariat en vertu de la *Loi sur la protection des renseignements personnels*. Bien que la Société de l'hôpital du Yukon soit régie par la *LPRPDÉ*, la plainte a été initialement déposée en vertu de la *Loi sur la protection des renseignements personnels*. Après discussion avec le requérant à cet effet, l'ancien commissaire est revenu sur sa décision de faire enquête sur la plainte. Les procédures légales ont été abandonnées le 21 février 2003.

Keith Vanderbeke c. Banque Royale du Canada

N° de dossier de la Cour fédérale du Canada : T-2185-02

Keith Vanderbeke a communiqué avec le Commissariat se plaignant que la Banque royale du Canada lui avait refusé l'accès à trois documents relatifs à une hypothèque commerciale pour laquelle il était personnellement le garant.

État de la situation

Dans la demande, le plaignant recherche particulièrement, entre autres choses, des ordonnances interprétatives relatives à la *LPRPDÉ* : une ordonnance selon laquelle une entreprise privée pourrait être une « personne identifiable » en vertu de la *LPRPDÉ*, jouissant corrélativement de droits d'accès ; et une ordonnance selon laquelle les documents bancaires de l'entreprise privée devraient être considérés comme des documents personnels lorsqu'une personne physique fournit une garantie personnelle au créditeur. Il n'est pas sûr que le traitement de cet aspect soit poursuivi car, entre autres, la partie de la demande apparemment présentée en vertu du paragraphe 14 de la *LPRPDÉ* vise à faire réviser de façon inappropriée les conclusions de l'ancien commissaire. Le seul défendeur légitime, en vertu du paragraphe 14 de la *LPRPDÉ*, est la Banque royale du Canada.

Partie III

Services de gestion

Le 1er avril 2002, le Commissariat à la protection de la vie privée du Canada a cessé de partager les services de gestion avec le Commissariat à l'information du Canada, et a créé sa propre Direction de la gestion intégrée.

La Direction de la gestion intégrée fournit à la fois des conseils et des services de gestion intégrée dans les domaines de la finance, des ressources humaines, de la technologie de l'information et des services administratifs aux cadres supérieurs et au personnel du Commissariat.

Tel qu'il est mentionné dans la préface, le Comité des opérations gouvernementales et des prévisions budgétaires a relevé un certain nombre de problèmes sérieux liés à certains de ces secteurs, au cours de son enquête relativement aux opérations du Commissariat. En outre, le Commissariat a fait l'objet d'examens menés à la fois par le Bureau de la vérificatrice générale du Canada et la Commission de la fonction publique du Canada.

J'ai l'intention d'utiliser les résultats de ces examens pour m'assurer que le Commissariat est géré de façon à être imputable au Parlement, et observe les politiques et les règlements applicables au secteur public.

Au début de l'année fiscale 2002-2003, le budget du Commissariat était de 11,1 millions de dollars, le même que notre budget pour l'année précédente. Au cours de l'année, notre budget a connu un ajustement à la hausse de 773 000 $, principalement pour faire face à une augmentation de coûts juridiques associés avec la nouvelle politique de l'Analyse des facteurs relatifs à la vie privée fédérale, et aux augmentations reliées à la négociation collective, pour un budget total de 11,9 millions de dollars.

Nos dépenses ont totalisé 12,2 millions de dollars. Nous avons excédé la limite de notre budget de 240 000 $, en grande partie à cause des pratiques de la comptabilité d'exercice afin d'être conforme aux principes de comptabilité d'exercice du gouvernement fédéral.

Le Commissariat révise actuellement ses ressources financières, conjointement avec le Secrétariat du Conseil du Trésor, afin de s'assurer qu'il a des ressources dont il a besoin pour s'acquitter de ses obligations en vue de l'année 2003-2004, et au-delà en prévision de la mise en œuvre complète et finale de la *LPRPDÉ* le 1er janvier 2004.

Resources

1er avril 2002 – 31 mars 2003

	Dépenses globales ($)	Pourcentage du total
Loi sur la protection des renseignements personnels	5 208 588	43 %
Loi sur la protection des renseignements personnels et les documents électroniques	5 582 722	46 %
Services de gestion	1 367 778	11 %
Total	**12 159 088**	**100 %**

À noter que depuis mars 2003, il y a eu 103 employées à temps plein au Commissariat à la protection de la vie privée du Canada.

Dépenses détaillées[1]

1er avril 2002 – 31 mars 2003

	Loi sur la protection des renseignements personnels	*Loi sur la protection des renseignements personnels et les documents électroniques*	Services de gestion[2]	Total
Salaires et traitements	3 462 955	2 845 391	808 513	**7 116 859**
Cotisations au régime d'avantages sociaux des employés	657 386	595 000	240 220	**1 492 606**
Transports et communications	284 228	352 412	67 005	**703 645**
Information	25 649	315 406	34 592	**375 647**
Services professionnels	679 897	700 870	65 526	**1 446 293**
Locations	12 840	2 202	11 648	**26 690**
Réparations et entretien	8 607	41 249	5 447	**55 303**
Approvisionnements et fournitures	44 328	5 012	51 699	**101 039**
Achat de machines et d'équipements	29 100	725 180	83 128	**837 408**
Autres subventions et paiements	3 598	-	-	**3 598**
Total	**5 208 588 $**	**5 582 722 $**	**1 367 778 $**	**12 159 088 $**

Nota :

[1] Les dépenses totales correspondent aux comptes publics.

[2] À compter du 1er avril 2002, les Services de gestion font partie du Commissariat et leurs services ne sont plus partagés avec le Commissariat à l'information du Canada.

Au début de l'année fiscale 2002-2003, le budget du Commissariat était de 11,1 millions de dollars, le même que notre budget pour l'année précédente. Au cours de l'année, notre budget a connu un ajustement à la hausse de 773 000 $, principalement pour faire face à une augmentation de coûts juridiques associés avec la nouvelle politique de l'Analyse des facteurs relatifs à la vie privée fédérale, et aux augmentations reliées à la négociation collective, pour un budget total de 11,9 millions de dollars.

Nos dépenses ont totalisé 12,2 millions de dollars. Nous avons excédé la limite de notre budget de 240 000 $, en grande partie à cause des pratiques de la comptabilité d'exercice afin d'être conforme aux principes de comptabilité d'exercice du gouvernement fédéral.

Le Commissariat révise actuellement ses ressources financières, conjointement avec le Secrétariat du Conseil du Trésor, afin de s'assurer qu'il a des ressources dont il a besoin pour s'acquitter de ses obligations en vue de l'année 2003-2004, et au-delà en prévision de la mise en œuvre complète et finale de la *LPRPDÉ* le 1er janvier 2004.

Resources

1er avril 2002 – 31 mars 2003

	Dépenses globales ($)	Pourcentage du total
Loi sur la protection des renseignements personnels	5 208 588	43 %
Loi sur la protection des renseignements personnels et les documents électroniques	5 582 722	46 %
Services de gestion	1 367 778	11 %
Total	**12 159 088**	**100 %**

À noter que depuis mars 2003, il y a eu 103 employées à temps plein au Commissariat à la protection de la vie privée du Canada.

Dépenses détaillées[1]

1er avril 2002 – 31 mars 2003

	Loi sur la protection des renseignements personnels	*Loi sur la protection des renseignements personnels et les documents électroniques*	Services de gestion[2]	Total
Salaires et traitements	3 462 955	2 845 391	808 513	**7 116 859**
Cotisations au régime d'avantages sociaux des employés	657 386	595 000	240 220	**1 492 606**
Transports et communications	284 228	352 412	67 005	**703 645**
Information	25 649	315 406	34 592	**375 647**
Services professionnels	679 897	700 870	65 526	**1 446 293**
Locations	12 840	2 202	11 648	**26 690**
Réparations et entretien	8 607	41 249	5 447	**55 303**
Approvisionnements et fournitures	44 328	5 012	51 699	**101 039**
Achat de machines et d'équipements	29 100	725 180	83 128	**837 408**
Autres subventions et paiements	3 598	-	-	**3 598**
Total	**5 208 588 $**	**5 582 722 $**	**1 367 778 $**	**12 159 088 $**

Nota :

[1] Les dépenses totales correspondent aux comptes publics.

[2] À compter du 1er avril 2002, les Services de gestion font partie du Commissariat et leurs services ne sont plus partagés avec le Commissariat à l'information du Canada.